Per E-Mail an jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 29. März 2017

Stellungahme der IAB zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die IAB (Interactive Advertising Bureau) Switzerland Association ("IAB") ist der Interessenverband der digitalen Werbebranche in der Schweiz und Teil der IAB Europe. Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Vorentwurf des Datenschutzgesetzes ("VE-DSG"). In unserer Stellungnahme gehen wir exemplarisch und ohne Anspruch auf Vollständigkeit auf diejenigen Vorschläge des Vorentwurfs ein, welche für die digitale Werbung in der Schweiz besonders relevant sind.

Das Wichtigste in Kürze:

Datenschutz und Datensicherheit sind wichtige Grundlagen für den Erfolg von digitalen Werbeformen. Der grenzüberschreitende Austausch von Personendaten muss möglich bleiben, weshalb ein inhaltlich gegenüber der EU gleichwertiger Datenschutz zu erhalten ist. Das Schweizer Datenschutzgesetz (DSG) aus dem Jahr 1992 basiert auf allgemeinen Grundsätzen der Datenbearbeitung, die sich in der Praxis bewährt haben und die sich bisher auch erfolgreich auf digitale Sachverhalte anwenden liessen. Gemäss Beschluss der EU-Kommission vom 26. Juli 2000 verfügt die Schweiz über ein angemessenes Datenschutzniveau. Dieser Beschluss bleibt auch unter der ab 25. Mai 2018 verbindlichen EU Datenschutz-Grundverordnung (Verordnung EU 2016/679; DSGVO) weiterhin gültig. **Eine Teilrevision des DSG genügt, um den Herausforderungen der Digitalisierung zu begegnen und einen gegenüber der EU angemessenen Datenschutz zu erhalten.**

Für die Schweiz **im internationalen Verhältnis direkt verbindlich ist das (revidierte) Übereinkommen des Europarates (SEV 108)** zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Das Übereinkommen bedingt, wenn überhaupt, lediglich wenige Änderungen im DSG. Solange die Schweiz die SEV 108 einhält besteht auch für die EU kein Grund, auf den Angemessenheitsentscheid zurückzukommen und diesen zu revidieren. **Für eine Übernahme der in der DSGVO detailliert geregelten administrativen Pflichten bei der Datenbearbeitung sowie für hohe Bussen besteht in der Schweiz kein Anlass.**

Doch der VE-DSG übernimmt die Regulierungen der DSGVO nicht nur weitgehend, sondern verschärft diese gar noch in verschiedenen Belangen, die für die Online Werbebranche in der Schweiz sehr nachteilig wären. In dieser Stellungnahme weisen wir nur auf die wichtigsten dieser strengeren Regelungen hin, welche die Geschäftstätigkeit von Online-Dienstleistern und Betreibern digitaler Geschäftsmodelle in der Schweiz bedrohen. **Sämtliche Verschärfungen gegenüber den Regelungen der DSGVO sind aus dem VE-DSG zu entfernen.** Vor allem auf überschiessende Neben- und Administrativpflichten ist zu verzichten. Solche Pflichten erhöhen den Aufwand für die Schweizer Anbieter von Werbung, Cloud-Lösungen und anderen Dienstleistungen für digitale Geschäftsprozesse. Die Administrativpflichten stärken auch den Persönlichkeitsschutz der betroffenen Personen kaum. Um die Attraktivität des Dienstleistungsstandorts Schweiz zu erhalten, sind Pflichten und Einschränkungen für Schweizer Anbieter zu vermeiden, welche sogar über das von der EU geforderte Mass hinausgehen.

Besonders standortschädlich und abzulehnen ist das vorgeschlagene Sanktionswesen mit neuen Straftatbeständen. Der Verzicht auf drakonische Sanktionen im Stile der DSGVO (Bussen bis zum höheren Betrag von EUR 20 Mio. oder 4% des letzten weltweit erzielten Jahresumsatzes) ist zwar zu begrüssen. Der VE-DSG setzt darauf, die Verletzung von administrativen Nebenpflichten neu als Straftatbestände auszugestalten. Ins Visier geraten damit die natürlichen Personen in der Schweiz, welche für die Datenbearbeitung in Unternehmen verantwortlich sind. Nur wenn sich diese nicht identifizieren lassen, soll subsidiär das Unternehmen mit maximal CHF 100'000.— gebüsst werden. Für global tätige Online-Plattformen ohne Niederlassung in der Schweiz wäre eine solche Busse im Vergleich zu einer Sanktion in der EU ein kleines Übel. Schweizer Unternehmen – besonders KMU – hingegen müssten ihre Mitarbeiter mit grossem Compliance-Aufwand schützen und würden sich im Zweifel für eine konservativere Methode der Datenbearbeitung entscheiden. **Im Ergebnis wäre der VE-DSG gut für Beratungsunternehmen und Anwaltskanzleien, nicht aber für innovative Unternehmen, die in der Schweiz datengestützte Geschäftsmodelle betreiben möchten.**

Im Einzelnen:

Die Auftragsdatenbearbeitung ist nicht unnötig zu erschweren (Art. 7 ff. VE-DSG):

Die Informationspflichten sind auf ein verhältnismässiges Mass zu beschränken. Die vorgesehenen Pflichten sind zu unbestimmt. Die aktive Information muss z.B. alle Angaben umfassen, die für die betroffene Person "erforderlich" sind (Art. 13 Abs. 2 VE-DSG). Längere Datenschutzerklärungen bedeuten nicht automatisch eine bessere Information der betroffenen Person. Daher verfehlt die Informationspflicht das Regelungsziel der Stärkung von Kontrollmöglichkeiten der Betroffenen. Die sehr weit formulierte Informationspflicht widerspricht dem risikobasierten Ansatz, wie sie der Vorentwurf im Rahmen der Transparenzanforderung gemäss Art. 4 VE-DSG vorsieht.

Die Pflicht zur Information über die Identität und Kontaktangaben der Auftragsbearbeiter ist überschiessend (Art. 13 Abs. 4 VE-DSG). Der Verantwortliche müsste die betroffene Person, z.B. bei jedem Wechsel des Werbe- oder IT-Dienstleisters, über die Identität und Adresse des neuen Anbieters informieren. Diese Information erhöht den Datenschutz und die Datensicherheit für die betroffene Person nicht, sondern führt zu einer kontraproduktiven Informationsflut. Die Information ist zudem in einer arbeitsteiligen, digitalen Geschäftswelt nicht praktikabel. Weder die SEV 108 noch die DSGVO verlangen die Angabe der Identität der Auftragsbearbeiter. Es ist nicht einzusehen, weshalb sich die Schweiz freiwillig einen massiven Standortnachteil auferlegen sollte.

Die Pflicht zur permanenten Datenüberprüfung ist in der Praxis nicht erfüllbar (Art. 4 Abs. 5 und Art. 19 Bst. b VE-DSG). Vor allem Auftragsbearbeiter sind von der Datenquelle zu weit entfernt, als dass sie Änderungsbedarf an den von ihnen bearbeiteten Daten erkennen können. Die Tätigkeit des Auftragsbearbeiters erfolgt immer im Auftrag des Verantwortlichen. Daher kann höchstens der Verantwortliche für die Richtigkeit der zur Verfügung gestellten Daten sorgen.

Auf strafrechtlich sanktionierte Informationspflichten des Auftragsbearbeiters gegenüber Datenempfängern ist zu verzichten (Art. 19 Bst. a VE-DSG). Daten werden tagtäglich angepasst, ergänzt oder gelöscht, weil die Daten nicht mehr notwendig sind oder an Relevanz verloren haben. Beispiele dafür sind die Archivbereinigung, der Abschluss der Leistungserbringung, die Begleichung der offenen Forderung durch den Kunden oder die Auflösung einer Geschäftsbeziehung. Es ist unverhältnismässig, wenn der Verantwortliche und der Auftragsbearbeiter in allen Fällen einer Berichtigung, Löschung oder Vernichtung von Daten alle Datenempfänger nachinformieren müssen. Die Informationspflicht ist auf Fälle zu begrenzen, in welchen die betroffene Person ein Begehren um Datenanpassung aufgrund schutzwürdiger Interessen gestellt hat. Die Mitteilung an Dritte soll höchstens dann erfolgen, wenn die betroffene Person dies aus berechtigten Gründen verlangt. Der Verantwortliche entscheidet über Zweck, Mittel und Umfang der Bearbeitung und ist damit auch in der Position, über den Bedarf für eine Datenanpassung zu befinden. Aus diesem Grund soll der Verantwortliche und nicht der Auftragsbearbeiter für die Mitteilung zuständig sein. So sieht es auch die EU vor (Art. 19 DSGVO).

Datenschutz-Folgenabschätzung, Privacy by Design und Privacy by Default sind keine Aufgaben des Auftragsbearbeiters (Art. 16 und 18 VE-DSG). Der Verantwortliche entscheidet über eine bestimmte Geschäftsaktivität und die damit zusammenhängende Datenbearbeitung. Die Pflichten zur Datenschutz-Folgenabschätzung, zur Sicherstellung des Datenschutzes durch Technik (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) setzen zu einem frühen Zeitpunkt in der Planung an. Der Auftragsbearbeiter ist in diese Entscheidungsprozesse meist nicht involviert. Hat der Auftragsbearbeiter einen entsprechenden Auftrag vom Verantwortlichen erhalten, verfügt er meist trotzdem nicht über alle relevanten Informationen. Die genannten Pflichten sind für den Auftragsbearbeiter daher kaum umsetzbar. Gleichzeitig stellen die Sanktionsdrohungen für den Auftragsbearbeiter unverhältnismässig hohe Risiken dar. Auch die EU beschränkt die genannten Pflichten auf den Verantwortlichen (Art. 25 und 35 DSGVO). Die Schweiz sollte die in der Schweiz ansässigen Dienstleister nicht gegenüber den EU-Anbietern benachteiligen. Sofern der Verantwortliche Schutzmassnahmen festlegt, wird er diese zudem auch vertraglich auf den Auftragsbearbeiter überbinden, soweit sie die Auftragsbearbeitung betreffen.

Die Einwilligungsvoraussetzung für eine Unterbeauftragung ist nicht praktikabel (Art. 7 Abs. 3 VE-DSG). In einer arbeitsteiligen Welt muss der Auftragsbearbeiter flexibel und zeitnah Unteraufträge vergeben können (z.B. eine Marketingagentur für die verschiedenen Elemente und Teilleistungen einer Kampagne). Er gewährleistet dabei gegenüber seinem Auftraggeber die Einhaltung der Pflichten durch die Unterauftragnehmer. Eine Pflicht zur vorgängigen Einholung der Einwilligung durch den Verantwortlichen ist praxisfern und nicht notwendig.

Der Auslandtransfer ist nicht unnötig zu verzögern und zu erschweren (Art. 5-6 VE-DSG):

Die zahlreichen Melde- und Genehmigungspflichten für die Bekanntgabe ins Ausland sind unverhältnismässig und fördern den Datenschutz nicht. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) würde zahlreiche für ihn kaum relevante Meldungen erhalten. Solche Mitteilungen bewirken für die betroffenen Personen keinen stärkeren Schutz. Die verpflichteten Verantwortlichen und Auftragsbearbeiter müssten in ihren Meldungen an den EDÖB unnötigerweise Geschäftsgeheimnisse offenbaren (z.B. betreffend hängiger ausländischer Verfahren). Für die Verpflichteten bestehen dabei unverhältnismässige Risiken, da die übermittelten Informationen dem Öffentlichkeitsgesetz unterliegen können. Ein Auftragsbearbeiter wird zudem nur auf Auftrag und Instruktion des Verantwortlichen tätig. Es ist der Verantwortliche, welcher die beauftragten Bearbeitungen als Teil seiner Geschäftsaktivität plant und über die erforderlichen Informationen verfügt. Es macht für eine zeitnahe Benachrichtigung und Aktivierung des EDÖB keinen Sinn den Auftragsbearbeiter für Praktiken in die Pflicht zu nehmen, die der Verantwortliche alleine bestimmt. Für einen Schweizer Cloud-Anbieter oder Werbe-Dienstleister, der von seiner Kundin ausserhalb Europas Daten erhält und speichert bzw. bearbeitet, ist unter der vorgeschlagenen Regelung zudem nicht klar, ob er für den Re-Export der Daten in das Land der Kundin eine neue vertragliche Grundlage (im Sinne von Abs. 3) benötigt. Die Bussendrohung stellt für den Auftragsbearbeiter eine unzumutbare Unsicherheit dar. Die strafrechtlich sanktionierten Melde- und Genehmigungspflichten sind insbesondere für Auftragsbearbeiter zu löschen.

Die vorgesehene Frist von sechs Monaten (anstelle der bis anhin 30 Tage) zur Prüfung von standardisierten Garantien und unternehmensinternen verbindlichen Vorschriften ist kontraproduktiv. Viele Anbieter können nicht so lange auf einen Bescheid warten und werden sich auf eine andere Basis für den Auslandtransfer stützen oder die geplante Aktivität aufgeben. Diese Frist ist für den EDÖB nicht einmal verbindlich, was zu einer unzumutbaren Rechtsunsicherheit und einem Nachteil für Schweizer Anbieter führt. Es ist zudem nicht einzusehen, warum bei spezifischen Garantien der EDÖB nur informiert werden muss, bei standardisierten Garantien aber eine langwierige Vorprüfung vorgeschrieben ist. Gerade standardisierte Garantien sowie unternehmensinterne verbindliche Vorschriften haben das Potential zur Entwicklung von wichtigen Best Practices. Davon profitieren wiederum die betroffenen Personen. Vorbildliche Anbieter, die für ihre Branche solche Standards durch regen Gebrauch etablieren möchten, sollen nicht durch unverhältnismässig lange Prüffristen des EDÖB blockiert werden.

Das DSG soll die Datenbekanntgabe auch im Zusammenhang mit einem Vertrag im Interesse der betroffenen Person erlauben. Die Bekanntgabe ins Ausland ist ausnahmsweise erlaubt, wenn die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten des Vertragspartners handelt. Unter der DSGVO ist die Bekanntgabe auch für den Abschluss oder die Erfüllung eines bloss im Interesse der betroffenen Person geschlossenen Vertrages möglich (Art. 49 Abs. 1 Bst. c DSGVO). Die Schweiz soll diese erweiterte Ausnahme den eigenen Anbietern nicht vorenthalten.

Auf unverhältnismässige Anforderungen an das Profiling ist zu verzichten (Art. 3 Bst. F und Art. 23 Abs. 2 Bst. d VE-DSG):

Informations- und Anhörungspflichten sollen auf automatisierte Entscheide mit erheblichen Auswirkungen beschränkt werden. In einem ersten Schritt ist der Begriff des Profiling einzuschränken auf die automatisierte Auswertung von personenbezogenen Daten, deren Ergebnis wiederum Personendaten sind. Dies sieht auch die DSGVO vor (Art. 4 Abs. 4 DSGVO). Profiling an sich hat für die betroffene Person kaum direkte Auswirkungen. Rechtliche Anforderungen sollen daher, wenn überhaupt, nur an die Verwendung der Ergebnisse anknüpfen, z.B. für automatisierte Entscheide. Erfasst wären aber potentiell sehr viele Routineverfahren, die im Rahmen der fortschreitenden Digitalisierung aus Effizienzgründen automatisiert werden, z.B. Prozesse zur Vertragsabwicklung. Die zusätzlichen administrativen Hürden für die Verpflichteten sollen in einem angemessenen Verhältnis zum Schutzbedürfnis der betroffenen Personen stehen. Die Pflichten bei automatisierten Einzelfallentscheiden sind daher in einem zweiten Schritt auf Entscheide zu beschränken, welche unmittelbare und erhebliche Auswirkungen auf die Persönlichkeitsrechte der betroffenen Person haben. Das DSG soll zudem weitere Ausnahmen von den Pflichten bei automatisierten Einzelfallentscheiden aufnehmen, wie dies auch die EU vorsieht (Art. 22 DSGVO). Darunter fallen z.B. Entscheidungen, die für den Abschluss oder die Erfüllung von Verträgen mit der betroffenen Person erforderlich sind.

Der Geheimnisschutz ist auf Berufe mit spezialgesetzlicher Schweigepflicht und eine berechtigte Geheimniserwartung einzuschränken (Art. 52 VE-DSG):

Eine Geheimhaltungspflicht soll nur greifen bei beruflichen Schweigepflichten, die unabhängig von Art. 52 VE-DSG bestehen. In den spezialgesetzlich erfassten Berufszweigen (z.B. Arzt, Anwalt) ist für alle Beteiligten klar, dass eine besondere Vertraulichkeit notwendig ist, z.B. für Patientendaten. Für viele andere Geschäftsfelder, die standardmässig Personendaten erfassen und bearbeiten (z.B. Online-Händler, Werbe-Dienstleister etc.), ist dies nicht der Fall. Früher oder später können praktisch alle Berufszweige mit geheimen Personendaten in Berührung kommen. Die vorgeschlagene Regel schliesst Anbieter damit weitgehend von jeglicher Nutzung der beschafften Daten aus. Die Bussendrohung für derart weit gefasste Pflichten ist unverhältnismässig. Sie ist zu beschränken auf berufliche Schweigepflichten, die ein anderes Gesetz vorschreibt. Wie bei anderen beruflichen Geheimnispflichten, muss eine Befreiung durch die Aufsichtsbehörde möglich sein.

Die Ausweitung des Geheimnisschutzes auf alle Personen, welche geheime Daten kommerziell bearbeiten ist überschiessend. Nicht einmal die EU sieht eine derart strenge Regelung vor. Dienstleister im Bereich personalisierter Online-Werbung, wie etwa Betreiber von Werbenetzwerken, könnten solche Dienstleistungen kaum mehr in der Schweiz anbieten. Die Sanktionsdrohung wäre ein weiterer massiver Standortnachteil für die Schweiz.

Nur diejenigen geheimen Daten sind zu schützen, für die der Geheimnisherr auch eine berechtigte Erwartung an die Geheimhaltung hat. Sofern zwischen dem Geheimnisherrn (d.h. der betroffenen Person) und dem Bearbeiter als Geheimnisträger z.B. eine vertragliche Grundlage für die Bearbeitung besteht, soll auch die Bearbeitung und entsprechende Offenlegung möglich sein.

Missbrauchspotential beim Auskunftsanspruch ist zu vermeiden (Art. 20 VE-DSG):

Der Auskunftsanspruch ist auf ein verhältnismässiges Mass an Daten zu beschränken. Die vorgesehene Auskunftspflicht umfasst alle Angaben zur Aufbewahrungsdauer, die Identität und Kontaktdaten aller Auftragsbearbeiter, das Ergebnis, Zustandekommen und die Auswirkungen von Entscheidungen, die auf irgendeiner Art von Datenbearbeitung beruhen. Dieser sehr weit gefasste Anspruch eröffnet Missbrauchspotential: Querulatorische Gesuche oder Anfragen zu datenschutzfremden Zwecken werden zunehmen. Das vorgeschlagene Auskunftsrecht geht weit über das verhältnismässige Mass und die Regelung der DSGVO hinaus. Die DSGVO beschränkt z.B. den zusätzlichen Anspruch auf Auskunft bei automatisierten Einzelfallentscheiden auf Fälle, in denen besonders schützenswerte Personendaten bearbeitet werden oder der Entscheid eine rechtliche Wirkung oder andere erhebliche Beeinträchtigung für die betroffene Person hat. Der ufer- und voraussetzungslose Auskunftsanspruch im VE-DSG steht in einem Missverhältnis zur Belastung der Auskunftspflichtigen. Aufgrund der vorgesehenen Bussendrohung, können Bearbeiter auch missbräuchliche Anfragen faktisch nicht mehr zurückweisen.

Für Auskunftsansprüche ist ein Kostenersatz vorzusehen. Ohne den Ausschluss des DSG in hängigen Zivilprozessen und laufenden Strafverfahren (Art. 2 Abs. 2 VE-DSG) eröffnet der Vorentwurf weiteres Missbrauchspotential: Mittels Auskunftsbegehren kann eine Verfahrenspartei kostenlos umfangreiches Beweismaterial für datenschutzfremde Zwecke beschaffen. Damit lassen sich z.B. die im Zivilprozess bestehenden Anforderungen für Editionsbegehren umgehen. Querulatorische oder wiederholte Anfragen können grosse Ressourcen binden. Ohne Kostenersatz geht das Risiko einseitig zu Lasten der Auskunftspflichtigen. Staatliche Behörden können bei einer Auskunft nach dem Öffentlichkeitsgesetz einen Kostenbeitrag verlangen. Selbst die DSGVO sieht zumindest bei wiederholten Anfragen den Kostenersatz vor (Art. 15 Abs. 3 DSGVO).

Selbstregulierung ist zu fördern und nicht zu verordnen (Art. 8-9 VE-DSG):

Nur Empfehlungen der guten Praxis aus der jeweiligen Branche selbst sind zielführend. Das DSG soll die Selbstregulierung in Eigeninitiative der jeweiligen Branchen fördern. Die Kompetenz dazu muss bei den interessierten Kreisen liegen, nicht beim EDÖB. Die Befugnisse des EDÖB zur Ausarbeitung und Genehmigung von Empfehlungen sind zu weitgehend und können zu praxisfernen Alleingängen führen. Nicht praktikable Empfehlungen schwächen den Datenschutz eher, als dass sie die Persönlichkeitsrechte der betroffenen Personen wirksam schützen. Erfahrungen mit Schweizer Selbstregulierungen haben gezeigt, dass echte Brancheninitiativen am wirksamsten sind. Auch der erläuternde Bericht nennte als Erfolgsbeispiele (S. 53) die Verhaltenskodizes der Brancheninitiative des Schweizerischen Verbandes der Telekommunikation für verbesserten Jugendmedienschutz in den neuen Medien und zur Förderung der Medienkompetenz in der Gesellschaft sowie den Code of Conduct Hosting der Swiss Internet Industry Association simsa.

Die freiwillige Benennung eines betrieblichen Datenschutzbeauftragten zeigt die Erfüllung der Sorgfaltspflichten des Unternehmens. Es ist richtig, dass die Schweiz auf die zwingende Benennung eines betrieblichen Datenschutzbeauftragten verzichtet. Das DSG soll aber Unternehmen, die freiwillig eine solche Sorgfaltsmassnahme ergreifen, von gewissen Pflichten entbinden. Die mit der Einsetzung eines betrieblichen Datenschutzbeauftragten gezeigte Sorgfalt ist zudem bei allfälligen Sanktionsbemessungen zu berücksichtigen.

Meldepflicht bei Datenschutzverletzungen muss verhältnismässig sein (Art. 17 VE-DSG):

Die Meldepflicht ist auf Datenschutzverletzungen mit erhöhtem Risiko für eine Vielzahl von Personen zu beschränken. Anders als in der EU, stellt der Wortlaut des Schweizer Vorentwurfs alle unbefugten Datenschutzbearbeitungen unter die Meldepflicht. Aus Gründen der Verhältnismässigkeit soll die Meldepflicht nur in Fällen eines Datenverlusts, einer unbefugten Offenlegung oder eines unbefugten Datenzugangs mit erhöhtem Risiko für die Persönlichkeitsrechte einer grösseren Zahl von betroffenen Personen greifen. Andernfalls rechtfertigen sich das Einschalten und Aktivwerden des EDÖB nicht. Die Verpflichteten sollen die dazu nötige Einschätzung der Risiken und Anzahl Betroffener nach sorgfältigen Massstäben aber in eigenem Ermessen durchführen können. Eine Meldung soll ohne unnötige Verzögerung erfolgen, wobei sachliche Gründe (z.B. Massnahmen zur Schliessung des Lecks, zur technischen Untersuchung etc.) eine Verzögerung rechtfertigen können.

Zu weitgehend ist auch die Meldepflicht an Dritte. Der Vorentwurf enthält die Schweizer Besonderheit, wonach jeder Verantwortliche und Auftragsbearbeiter allfällige Drittempfänger der Daten über Verletzungen des Datenschutzes informieren muss. Diese Mitteilung hat unabhängig davon zu erfolgen, ob eine Meldung an den EDÖB oder an die betroffene Person notwendig ist. Die EU sieht keine solche Pflicht vor (Art. 19 DSGVO). Diese Mitteilung beinhaltet ein enormes Potential zur Rufschädigung. Es ist nicht einzusehen, weshalb die Schweiz derartige Verschärfungen einführen soll, die keine Erhöhung des Datenschutzes aber massive administrative Aufwendungen für Verantwortliche und Auftragsbearbeiter bewirken.

Auf unverhältnismässige Sanktionen einseitig zulasten der Schweizer Anbieter ist zu verzichten (Art. 50-53 VE-DSG):

Der Verzicht auf hohe Bussen führt nicht zum Verlust des Angemessenheitsbeschlusses der EU. Das SEV 108 verlangt lediglich die "wirksame" Umsetzung (Art. 4 Abs. 1 und 3 Bst. a SEV 108) und "geeignete" Sanktionen (Art. 10 SEV 108). Das DSG muss keine hohen Bussen für Administrativpflichten vorsehen, um diesen Anforderungen gerecht zu werden. Die Verfügungskompetenz des EDÖB und die Sanktion bei Widerhandlungen gegen rechtskräftige Verfügungen (Art. 292 StGB) reichen als wirksame Durchsetzungsmassnahmen aus.

Die selbständige Sanktionierung von Administrativpflichten stärkt den Datenschutz nicht und ist unverhältnismässig. Die zahlreichen selbständig sanktionierten, administrativen Pflichten (Art. 50 und 51 VE-DSG) erhöhen den administrativen Aufwand und das finanzielle Risiko für Schweizer Anbieter. Diese Pflichten bleiben aber weitgehend ohne direkte Wirkung für den Schutz der Persönlichkeitsrechte der betroffenen Personen.

Hohe Schweizer Bussen bedrohen einseitig Schweizer Anbieter. Die vorgeschlagene Sanktionsregelung bedeutet für in der Schweiz ansässige KMU eine stärkere finanzielle Belastung, als für grosse, internationale Konzerne: Für internationale Anbieter ohne Schweizer Niederlassung ist der Anreiz grösser, die natürliche Person nicht identifizierbar zu halten. Für Schweizer Anbieter liesse sich demgegenüber regelmässig leichter feststellen, wer als natürliche Person zur Verantwortung gezogen werden kann. Damit sind die Risiken gerade für Geschäftsführer und leitende Angestellte von Schweizer Unternehmen grösser als für internationale Konkurrenten. Eine grosse Rechtsunsicherheit für die verpflichteten Unternehmen besteht zudem aufgrund fehlender Harmonisierung und sehr unterschiedlicher datenschutzrechtlicher Erfahrung der zuständigen kantonalen Strafbehörden.

Die Ausweitung des Strafkatalogs widerspricht der Schweizer Rechtstradition. Unter dem geltenden DSG sollen Datenschutzverstösse nur ausnahmsweise mit strafrechtlichen Sanktionen geahndet werden (Botschaft des Bundesrates vom 23. März 1988 zum DSG, BBl 1988 II 413, 484). In der Schweizer Rechtstradition ist nicht zwingend eine Androhung von Strafen notwendig, damit gesetzliche Verpflichtungen als verbindlich aufgefasst werden. Den Verpflichteten drohen bei Nichtbefolgen der Administrativpflichten an sich bereits regelmässig Rechtsnachteile, z.B. wegen fehlender Nachweise in einem Verfahren. Zudem sind die administrativen Pflichten im Vorentwurf sehr unbestimmt (z.B. die Dokumentationspflicht), was eine Bestrafung rechtsstaatlich problematisch macht. Die Ausweitung des Sanktionskatalogs für Administrativpflichten schadet auch dem offenen und zielgerichteten Dialog zwischen Datenbearbeitern und

dem EDÖB. Für die Berücksichtigung der Anliegen der Werbebranche zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung.

Mit freundlichen Grüssen

David Burst
Präsident

Rolf Auf der Maur
Vorstand, Ressort Recht

Der Anschluss ans Leben

1892–2017

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Brugg, 31.03.2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt IBB ComNet AG gerne wahr.

IBB ComNet AG ist ein Anbieter von Telekommunikationsnetzinfrastrukturen und -dienstleistungen. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung"

durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-

Shop" nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden."). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen *für die Wirtschaft und die Gesellschaft erläutert werden.*

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands."[2]

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen."[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichen-

---

1 Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

2 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

3 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

den Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80'000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365" für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da

---

4 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

5 Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

> sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei."[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40'000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10'000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5'000 – 10'000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5'000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7'500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5'000 – 30'000
Privacy by Default	1 – 40 Stunden		500 – 5'000
Betriebliche Datenschutzbeauftragter		500 – 2'000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5'000

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1'532'160'000, resp. im Durchschnitt von CHF 2'520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die

---

6 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

7 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

8 *In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14'000 – 149'000 geschätzt.* Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

9 608'000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen."[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

---

10 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (neu)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*" grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (Beispiel: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz", Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis" abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten". Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten" konsumiert. Der Begriff des „Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil" des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling" gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish" versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage" eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling" verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist" gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag" (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag" wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter").
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten" aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit" einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig", „freiwillig und eindeutig", „ausdrücklich" und die Abgrenzung zur blossen „Einwilligung" (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig", „eindeutig" oder „ausdrücklich" auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise" völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste.
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen.	**Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen.
[5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	**Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen" Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1**: Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche" Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen" reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish" erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant" zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves" und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4. [3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten“ und „Persönlichkeitsprofilen“. Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. *Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der* Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d):** Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat". Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere:	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit.
a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;	**Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert.
b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist;	**Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. [3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle [1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. [2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen [1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. [2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. [3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1" (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 *Widerspruch gegen die Bekanntgabe von Personendaten* [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen. [2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen". Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung *angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise* vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen" und ersetzen mit „seine Untersuchungen". Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500'000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1'000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5'000 – 30'000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten" wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom … *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom…. *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom …… *Art. 114 Bst. f* Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …… *Art. 243 Abs. 2 Bst. d* [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 ... Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Philippe Ramuz
Geschäftsleiter Netz-Dienstleistungen

Ralph Zebert
Geschäftsleiter Energie-Dienstleistungen

Bundesrätin Simonetta Sommaruga
Eidgenössisches Justiz- und Polizeidepartement EJPD

per E-Mail an jonas.amstutz@bj.admin.ch

Bern, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

ICTswitzerland nimmt die Gelegenheit wahr, sich Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) zu äussern. Gerne unterbreiten wir Ihnen nachfolgend unsere Stellungnahme.

ICTswitzerland ist die Dachorganisation der Verbände sowie der Anbieter- und Anwenderunternehmen von Informations- und Kommunikationstechnologien (ICT). 27 Grossunternehmen und 21 ICT-Verbände sind an den Dachverband angeschlossen (Mitgliederliste: ictswitzerland.ch/organisation/mitglieder). ICTswitzerland vertritt die Interessen der ICT-Wirtschaft gegenüber der Öffentlichkeit und den Behörden, bezweckt die Förderung und Weiterentwicklung der Branche, fördert die führende Position der Schweiz im Bereich Forschung und Entwicklung und den Nachwuchs von qualifizierten ICT-Fachkräften. Die ICT-Branche ist mit einer Bruttowertschöpfung von CHF 28 Mrd. (2014) die sechstgrösste Wirtschaftsbranche der Schweiz.

1. Grundlegende Bemerkungen

Die Schweizer ICT-Wirtschaft unterstützt ein wirksames und modernes Datenschutzgesetz in der Schweiz – dies schafft Vertrauen zwischen Kunden und Anbietern. Akzeptanz und Vertrauen der Nutzer in den Datenschutz sind zentrale Voraussetzungen für die Fortentwicklung der digitalen Wirtschaft. Für die Wirtschaft sind Rechts- und Investitionssicherheit und eine Regulierung, die Raum für Innovation und wirtschaftliche Entwicklung lässt, von grosser Bedeutung.

Angesichts der dynamischen internationalen Entwicklung im Bereich des Datenschutzes ist es für die Schweiz zentral, dass sie den Zugang zum internationalen Markt nicht unnötig einschränkt. Damit der Schweizer Datenschutz insbesondere auch von der EU weiterhin als äquivalent angesehen werden kann, reicht es jedoch, wenn sie die grundlegenden Garantien einhält (vgl. Erw. 104 EU-DSGVO; US-EU Privacy Shields). Die Schweiz

muss sich zudem an der verbindlichen Konvention 108 des Europarats[1] und der Richtlinie (EU) 2016/680[2] orientieren.

Im Rahmen der internationalen Vorgaben ist ein Maximum an Flexibilität für den Schweizer Standort zu erhalten. Die Wirtschaft soll nicht mit unnötigem administrativem und finanziellem Aufwand belastet werden. Ein «Swiss Finish», der über die internationalen Standards oder gar über die EU Datenschutz-Grundverordnung (EU-DSGVO) hinausgeht, ist zu vermeiden. Dieser wäre aus einer gesamtheitlichen Sicht kontraproduktiv, weil solche Schweizer Besonderheiten einen einheitlichen internationalen Datenraum verhindern und damit auch zulasten der Schweizer Unternehmen wettbewerbsverzerrend wirken würden. Vor allem wirken sich überschiessende und im Geschäftsalltag nicht praktikable Regulierungen innovationshemmend aus und können der Wettbewerbsfähigkeit von Schweizer Unternehmen nachhaltig schaden.

ICTswitzerland ist überzeugt, dass die Schweiz einen wirksamen Datenschutz und die notwendige Äquivalenz mit einer schlanken Gesetzgebung erreichen kann. In Zusammenarbeit mit der branchenübergreifenden Arbeitsgruppe Datenschutz bei economiesuisse hat ICTswitzerland in mehreren Kapiteln Anpassungsbedarf identifiziert, der im Folgenden dargestellt wird.

2. Zweck (Art. 1)

Die Zweckbestimmung ist anzupassen. Gerade auch unter Berücksichtigung der Strategie «Digitale Schweiz» des Bundesrates ist der Zweck um «die Förderung des freien Verkehrs der Personendaten» zu ergänzen. Dies entspricht dem Ziel des erläuternden Berichts, dass durch die Datenschutzgesetzrevision «die Wettbewerbsfähigkeit der Schweiz gewährleistet und verbessert werden [soll], namentlich indem die Bekanntgabe von Daten ins Ausland erleichtert wird». Eine entsprechende Zielsetzung kennt auch die europäische Verordnung.

3. Geltungsbereich (Art. 2)

Berücksichtigung bereichsspezifischer Datenschutzbestimmungen
In verschiedenen Bereichen (z.B. in der Humanforschung) bestehen spezielle Bestimmungen zu datenschutzrechtlichen Fragen. Diese sind teilweise auf Verordnungsebene festgeschrieben. Es ist für die betroffenen Unternehmen zentral, dass sie sich weiterhin auf die entsprechenden Regelungen verlassen können. Es sollte festgehalten werden, dass Spezialbestimmungen im Datenschutzrecht den Regelungen des DSG vorgehen bzw. dass der Grundsatz «lex specialis» umfassend zu verstehen ist.

[1] SEV Nr.108 – Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten
[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

Kein Schutz für juristische Personen
Die Abschaffung des Datenschutzes für Unternehmen analog der EU-DSGVO und Konvention 108 wird begrüsst. Dieser hat bis in der Praxis kaum eine Rolle gespielt. Einzelunternehmen und Mitglieder von Personengesellschaften, die im Handelsregister eingetragen sind, sind jedoch weiterhin vom Schutz umfasst. Es wird angeregt, dass hier dieselbe Regelung zum Geltungsbereich wie für juristische Personen gelten sollte.

Neues Missbrauchspotential beim Auskunftsrecht
Der VE-DSG sieht neu vor, dass das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren zur Anwendung gelangen soll. Dieser erweiterte Geltungsbereich birgt erhebliches Missbrauchspotential beim Auskunftsrecht (Beweisbeschaffung über die zivilprozessualen Editionsrechte hinaus). Es braucht griffige Mechanismen, welche dem Rechtsmissbrauch oder der nicht vorgesehenen Anwendung dieser Bestimmung im Zivilprozess oder im Strafverfahren entgegenstehen (vgl. Ziff. 11).

Regelung des räumlichen Anwendungsbereichs / IPR
Im VE-DSG fehlt eine Regelung zum räumlichen Anwendungsbereich des Gesetzes. Von wirtschaftlicher Seite her besteht der Wunsch, den räumlichen Anwendungsbereich nicht übermässig auszudehnen und damit den Status quo beizubehalten. Dies bedarf einer gleichzeitigen Anpassung der entsprechenden Regelung im Bundesgesetz über das Internationale Privatrecht (IPRG), damit der Geltungsbereich des Schweizerischen Datenschutzgesetzes in räumlicher Hinsicht relativiert werden kann.

4. Begriffe (Art. 3)

Definition der Personendaten
Art. 3 lit. a VE-DSG sieht keine Definition der Bestimmbarkeit vor. Es ist zu konkretisieren, was unter «bestimmbaren Personendaten» zu verstehen ist. Zudem ist wie im geltenden Recht klarzustellen, dass mit dem Begriff «Daten» stets Personendaten gemeint sind.

Einschränkung der Definition der besonders schützenswerten Personendaten
Die Ausweitung des Begriffs der «besonders schützenswerten Personendaten» auf die entsprechenden Definitionen der genetischen und biometrischen Daten geht zu weit. Der Wortlaut widerspricht den Erläuterungen im Bericht: Angedacht war die Erfassung von Daten, welche zum Zweck bearbeitet werden, eine natürliche Person eindeutig zu identifizieren. Dies entspricht auch der Stossrichtung der Konvention 108. Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Einschränkung der Definition des Profiling
Die Definition des Begriffs «Profiling» ist im VE-DSG sehr breit gefasst und geht deutlich über die entsprechende Regelung der EU hinaus. In der EU-DSGVO hängt die Zulässigkeit des Profilings von der Wahrnehmung der betroffenen Interessen ab. Nur in Fällen, in denen das Profiling Teil einer automatischen Entscheidung wird und rechtliche Wirkung erzeugt, gelten andere Vorschriften. Der VE-DSG vermischt die beiden Institute: Erfasst ist auch das «menschliche», d.h. manuelle Profiling (z.B. eine schriftliche

Mitarbeiterbeurteilung oder die Alterskapitalberechnung einer Versicherung) sowie nicht-personenbezogene Daten. Dies stellt eine unzulässige Ausweitung des Geltungsbereiches dar und steht damit im Widerspruch zu Art. 2 Abs. 1 VE-DSG.

Die Definition des Begriffes ist analog der EU-DSGVO auf die automatisierte Auswertung von Personendaten zu begrenzen. Zudem ist die Auswertung bzw. Analyse keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte auswirkt. Die Bestimmung sollte daher anstatt «Auswertung» analog der EU-DSGVO den Begriff «Bewertung» verwenden.

Einführung des betrieblichen Datenschutzbeauftragten
Es besteht der Wunsch, eine Regelung zur Bezeichnung eines betrieblichen Datenschutzbeauftragten auf freiwilliger Basis vorzusehen. Dies kann mit einer entsprechenden Erleichterung bei den Pflichten unter dem DSG verknüpft werden (vgl. Ziff. 8.2). In diesem Sinne ist auch eine Definition des betrieblichen Datenschutzbeauftragten erforderlich.

5. Grundsätze (Art. 4)

Klare Terminologien
Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zweckes unnötigerweise mit dem Zusatz der «klaren» Erkennbarkeit. Diese Anpassung an die Terminologie der EU-DSGVO ist in diesem Falle verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert damit auch Rechtsunsicherheit. Der Zusatz ist nicht erforderlich und zu streichen.

Dies gilt auch für den Begriff der «eindeutigen» Einwilligung von Art. 4 Abs. 6 VE-DSG. Damit wird lediglich wiederholt, was bereits heute unter dem risikobasierten Ansatz gilt. Der Zusatz ist ebenfalls wegzulassen. Auch wann eine Einwilligung «ausdrücklich» sein soll, ist nicht klar. Jedenfalls muss auch passives Verhalten als gültige Einwilligung gelten, damit weiterhin die im Massengeschäft unumgänglichen Allgemeinen Geschäftsbedingungen (AGB) verwendet werden können. Das Erfordernis der Einwilligung für das Profiling muss gänzlich gestrichen werden (vgl. Ziff. 13).

Keine Nachführungspflicht
Die permanente Nachführungspflicht geht zu weit und ist nicht praktikabel. Der 1. Satz von Art. 4 Abs. 5 VE-DSG ist entsprechend ersatzlos zu streichen.

6. Auslandtransfer (Art. 5, Art. 6)

Unnötige Wiederholung von Grundsätzen
Art. 5 Abs. 1 VE-DSG wiederholt bereits statuierte Grundsätze und ist im Kontext von Art. 5 verwirrend und überflüssig. Der Absatz ist deshalb zu streichen.

Keine Feststellung durch den Bundesrat
Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung würde besser durch den Verantwortlichen, gestützt auf eigene Abklärungen und Kenntnisse, erfolgen. Die Bestimmung ist im Sinne einer geringeren Einschränkung anzupassen.

6.1. Informations- und Genehmigungspflicht (Art. 5)

Unklare und widersprüchliche Kategorisierung der Garantien
Die Unterscheidung in Art. 5 Abs. 3 VE-DSG zwischen «spezifischen» und «standardisierten» Garantien ist unklar und macht aus Sicht der Praxis keinen Sinn. Erschwerend kommt hinzu, dass die standardisierten Garantien einer Genehmigung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bedürfen.

Auch Binding Corporate Rules (BCR) unterliegen der Genehmigungspflicht, diese stellen aber eine Untergruppe der spezifischen Garantien dar. Für diese wiederum ist jedoch nur eine Informationspflicht vorgeschrieben. Dies ist widersprüchlich. Es sollte lediglich zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden und die Pflichten entsprechend angepasst werden.

Berücksichtigung von Geheimhaltungsinteressen
Spezifische Garantien sind in der Regel in Verträgen enthalten. Es ist praxisfern und insbesondere im Zusammenhang mit dem Öffentlichkeitsgesetz (BGÖ) problematisch, wenn diese alle dem EDÖB vorgelegt werden müssen.

Keine Genehmigung durch den Beauftragten
Die Genehmigung von standardisierten Garantien oder verbindlichen unternehmensinternen Datenschutzvorschriften (BCR) durch den Beauftragten ist zu streichen. Die Genehmigungspflicht würde zu einem erheblichen Mehraufwand für die Unternehmen und gegebenenfalls zu Projektverzögerungen führen. Gleichzeitig trägt sie kaum etwas zum besseren Datenschutz bei, da das Unternehmen weiterhin selber in der Verantwortung steht. Ein grenzüberschreitender Datenfluss würde durch diese Regelung erheblich erschwert. Lediglich die EU-DSGVO (nicht die Konvention 108) sieht eine entsprechende Vorgabe vor. Hier besteht Raum für einen sich im Verhältnis zur EU-DSGVO differenzierenden Regelungsansatz.

Keine Informationspflicht bei Vorliegen standardisierter Garantien
Die pauschale Informationspflicht von Art. 5 Abs. 6 VE-DSG im Zusammenhang mit standardisierten Garantien bringt keinen Mehrwert. Es geht hier um bereits genehmigte oder anerkannte Garantien. Dies ist nicht einmal in der EU-DSGVO vorgesehen.[3] Die Bestimmung ist entsprechend zu streichen.

[3] Vgl. dazu EuGH-Entscheid Schrems und Entscheid der EU-Kommission vom 16.12.2016 (keine erneute Einwilligung im Einzelfall).

6.2. Ausnahmen (Art. 6)

Keine Einwilligung «im Einzelfall»
Die in Art. 6 Abs. 1 lit. a VE-DSG vorgesehene Ausnahme der «Einwilligung im Einzelfall» ist weder sinnvoll noch notwendig. Nach den allgemeinen Grundregeln reicht für wiederkehrende Sachverhalte bei gleichbleibender Erkennbarkeit und Erwartung eine einmalige Einwilligung. Der Zusatz «im Einzelfall» ist zu streichen. Dies gilt auch für die «Bekanntgabe im Einzelfall» (Art. 6 Abs. 1 lit. d VE-DSG).

Erweiterung der Ausnahme i. Zh. mit Verträgen
Die Ausnahmebestimmung von Art. 6 Abs. 1 lit. b VE-DSG ist mit der EU-DSGVO abzustimmen. Die Ausnahme ist auf diejenigen Fälle auszuweiten, in denen die betroffene Person nicht Vertragspartei ist, der betroffene Vertrag aber in ihrem Interesse ist oder zu ihren Gunsten abgeschlossen wurde.

Streichung Begriffe «Gericht» und «Verwaltungsbehörde»
Die Begriffe «Gericht» und «Verwaltungsbehörde» bei Art. 6 Abs. 1 lit. c VE-DSG sind zu streichen. Die Unterscheidung ist nicht erforderlich und es stellen sich schwierige Abgrenzungsfragen. Massgebend ist, dass die Datenbearbeitung zur «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen» erfolgt.

Keine Informationspflicht bei Vorliegen eines Ausnahmetatbestandes
Die in Art. 6 Abs. 2 vorgesehene Informationspflicht, trotz Vorliegen eines Ausnahmetatbestandes, ist unverhältnismässig und zu streichen. Eine entsprechende Bestimmung ist in der Konvention 108 nicht vorgesehen. Nebst zu erwartender hoher Anzahl an Meldungen wäre auch die Information des EDÖB über heikle Verfahren und (Geschäfts-)geheimnisse problematisch (BGÖ).

7. Auftragsdatenbearbeitung (Art. 7)

Keine Vergewisserungspflicht
Die in Art. 7 neu vorgesehene Vergewisserungspflicht führt zu massivem Mehraufwand beim Outsourcing der Datenbearbeitung. Es ist unklar, welche Pflichten dem Auftragsdatenbearbeiter auferlegt werden sollen. Die Vergewisserungspflicht widerspricht dem prinzipienbasierten Ansatz des VE-DSG und die Präzisierung ist gerade in Bezug auf projektspezifische Herausforderungen kontraproduktiv. Die Bestimmung ist zu streichen. Dies gilt auch für den letzten Satz von Absatz 2 bezüglich Präzisierung weiterer Pflichten des Auftragsbearbeiters durch den Bundesrat.

Reduzierte Anforderungen an die Einwilligung
Die Anforderung einer «schriftlichen» Zustimmung ist vor dem Hintergrund der heutigen Geschäftsprozesse, insbesondere auch aufgrund der komplexen Dienstleistungsverhältnisse, nicht praxistauglich. Eine dokumentierte Zustimmung reicht aus; Schriftlichkeit i.S.v. Art. 13 OR ist nicht erforderlich. Es ist eine technologieneutrale Präzisierung vorzunehmen, dass – dies auch im Einklang mit der Bestimmung in der EU – eine generelle Einwilligung für den Beizug von Sub-Auftragsdatenbearbeitenden und eine Information im konkreten Fall ausreicht.

8. Selbstregulierung (Art. 7, Art. 8, Neu)

8.1. Empfehlungen der guten Praxis (Art. 8)

Begrüssenswerte Selbstregulierung aber keine Empfehlungen des Beauftragten
Grundsätzlich sind Empfehlungen der guten Praxis in Anlehnung an das bestehende und bewährte Konzept der Selbstregulierung der Branchen zu begrüssen. Der wesentliche Vorteil liegt darin, dass so sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präsentiert werden können. Dazu müssen themenspezifische Wünsche der Branche tatsächlich in die Regelung einfliessen. Die im VE-DSG vorgesehene Kompetenz des EDÖB, Empfehlungen der guten Praxis auf eigene Faust auszuarbeiten, widerspricht aber dem Zweck des Instituts. Es fehlen Kontrollen und Rechtsschutzmechanismen. Entsprechend besteht die Gefahr, dass der EDÖB «falsche» oder unverhältnismässige Empfehlungen verabschiedet, ohne institutionelle Kontrolle. Aufgrund der Fiktion der Rechtmässigkeit von Art. 9 Abs. 1 VE-DSG würde er damit faktisch zum Gesetzgeber. Dem stünde verschärfend entgegen, dass eigene Empfehlungen der interessierten Kreise nur mittels Genehmigung durch den EDÖB festgelegt werden könnten. Unter der EU-DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Daraus ergibt sich, dass die Bestimmung der VE-DSG dahingehend anzupassen ist, dass die Initiative für Empfehlungen der guten Praxis von (Branchen-)Verbänden ausgehen muss. Dies würde der Tradition der Selbstregulierung entsprechen und brächte den Vorteil mit sich, dass solche Richtlinien von Experten mit starkem Bezug zur Praxis verfasst werden. Dies würde es ermöglichen, sachgerechte Lösungen zu entwickeln, bei denen der Beauftragte durch die Genehmigung immer noch das letzte Wort hat. Die genehmigten Empfehlungen der guten Praxis sind vom EDÖB zu publizieren.

Vermutung der Richtigkeit statt Fiktion / Geltung auch für Auftragsdatenbearbeiter (Art. 9)
Die Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung der Datenschutzvorschriften schliesst, ist ausserdem nicht zielführend. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig /unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.

8.2. Betrieblicher Datenschutzbeauftragter (NEU)

Einführung auf freiwilliger Basis gekoppelt mit Freistellung von Meldepflichten
Der VE-DSG verlangt richtigerweise nicht die breite Einführung eines betrieblichen Datenschutzbeauftragten. Das Institut eines betrieblichen Datenschutzbeauftragten sollte aber weiterhin vorgesehen werden. Dies als Option für die Unternehmen, kombiniert mit der Freistellung von allfälligen Meldepflichten gegenüber dem EDÖB (z.B. bei der Datenschutz-Folgenabschätzung). Ein betrieblicher Datenschutzbeauftragter könnte als zentrale Stelle die Pflichten für die Unternehmen oder ganze Unternehmensgruppen wahrnehmen. Damit liessen sich Doppelspurigkeiten vermeiden. Auch würde dadurch eine Anlaufstelle für Auskunftsbegehren geschaffen. Dies würde eine Flexibilisierung und gerade für grössere Unternehmen Erleichterungen mit sich bringen, ohne dass KMU belastet würden. Die betrieblichen Datenschutzbeauftragen sind auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen (z.B. bei Art. 15, 16 und 17 VE-

DSG). Die entsprechende Person darf jedoch im Rahmen von Sanktionen nicht übermässig exponiert werden (siehe hierzu Ziff. 14.3).

9. Daten einer verstorbenen Person (Art. 12)

Keine Regelung im DSG

Art. 12 VE-DSG erscheint im VE-DSG als Fremdkörper. Die Regelung könnte zu Rechtsunsicherheiten führen. Der Nachweis der persönlichen Beziehungen im Zusammenhang mit dem schutzwürdigen Interesse ist in der Praxis kaum zu erbringen. Für Geschäftsdaten bestehen gemäss spezialgesetzlichen Regelungen weitreichende legitime Dokumentations- und Archivierungspflichten, weshalb die pauschale Formulierung des Löschungsrechts nicht zielführend ist. Erben sind bereits durch die erbrechtliche Universalsukzession ausreichend legitimiert, geeignete, interessenwahrende Massnahmen vorzukehren. Die Bestimmung ist deshalb im VE-DSG zu streichen. Eine Regelung wäre an geeigneter Stelle (z.B. im ZGB) vorzusehen, dies aber zu einem späteren Zeitpunkt im Rahmen einer umfassenden Regelung in Bezug auf die Verfügung über Daten und nicht ausschliesslich aus einer datenschutzrechtlichen Sicht.

10. Pflichten (Art. 13 bis Art. 19)

Keine pauschale Anwendung

Die pauschale Anwendung der vorgesehenen Pflichten auf alle Geschäftsmodelle und Branchen ist nicht sachgerecht und wäre mit enormem Aufwand verbunden. Es gilt, ein gestuftes Modell vorzusehen: Strengere Bestimmungen wären dabei für Geschäftsmodelle vorzusehen, welche besonders sensible Datenbearbeitungen umfassen, wie dies typischerweise bei spezifischen Marketing-Dienstleistern und Data-Minern der Fall ist. Auch bei den Pflichten ist ein risikobasierter Ansatz vorzukehren. Zudem können branchenspezifische Regelungen weitergehende Pflichten vorsehen.

Erleichterungen für Unternehmensgruppen

Gleich strenge Regelungen für die interne Weitergabe von Daten in Konzernverhältnissen sind nicht verhältnismässig. Analog Art. 47 EU-DSGVO ist eine Bestimmung zu internen Datenschutzvorschriften für die erleichterte gruppeninterne Datenweitergabe in das DSG aufzunehmen. Dabei ist auch der Einsatz eines allfälligen internen Datenschutzbeauftragten zu berücksichtigen (vgl. Ziff. 8.2).

10.1. Informationspflichten (Art. 13)

Risikobasierte Transparenzpflicht als Leitlinie

Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen aufgrund des öffentlich-rechtlichen Charakters der Bestimmungen und den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Die vorgesehene massive Ausdehnung der Informationsmenge führt zu einer Überinformation der betroffenen Personen und würde sich damit kontraproduktiv auf die Transparenz auswirken. Die Regel muss grundsätzlich im Sinne einer risikobasierten Transparenzpflicht überarbeitet werden. Es sollte zudem explizit die Möglichkeit von standardisierten Informationen (z.B. mittels AGB oder

Erklärungen auf Websites) eingeführt werden. Dies auch deshalb, weil oft nicht klar ist, worüber genau informiert werden muss.

Konkret ist die Informationspflicht auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektiven) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person zu beschränken. Ausserdem ist klarzustellen, dass sich die Information – und damit auch die Richtigkeit und Vollständigkeit der Daten – auf den Zeitpunkt der Datenbeschaffung bezieht und nicht auf nachträgliche Änderungen. Dies schliesst auch eine Pflicht zur Nachinformation klar aus. Als Kontaktdaten des Verantwortlichen muss eine klare und definierte Funktionsbeschreibung ausreichen, da die natürliche Person innerhalb einer Funktion wechseln kann.

Präzise und einheitliche Terminologien
Unklar ist die Differenzierung zwischen «Beschaffung» und «Bearbeitung» und die in Abs. 3 verwendeten Begriffe «Dritte» sowie «Empfängerinnen und Empfänger». Es sollten präzisere und einheitliche Terminologien verwendet werden. Es ist auch fraglich, warum der Vorentwurf den Begriff «Beschaffung» statt wie in der EU-DSGVO vorgesehen «Erhebung» verwendet. Dadurch können sich (nachteilige) Abweichungen im Informationszeitpunkt ergeben.

Keine Mitteilung von Identität und Kontaktdaten der Auftragsdatenbearbeiter
Die Pflicht zur Mitteilung der Identität und der Kontaktdaten sämtlicher Auftragsdatenbearbeiter ist gegenüber dem EU-Recht klar überschiessend. Sie ist weder sinnvoll noch erforderlich. Die Offenlegung der oft für untergeordnete Tätigkeiten mandatierten Auftragsdatenbearbeiter ist nur mit unverhältnismässigem Aufwand zu bewerkstelligen und greift zudem in berechtigte eigene Datenschutzinteressen sowie Geschäftsgeheimnisse der Unternehmen ein. Schliesslich ist unklar, wann genau über was informiert werden muss. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist bereits Gegenstand von Art. 7 VE-DSG. Diese Zusatzanforderung ist zu streichen.

Keine Mitteilung bei indirekter Datenbeschaffung
Die vorgesehene Informationspflicht bei der indirekten Datenbeschaffung geht zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein. Das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus sind solche direkten Informationspflichten nicht erforderlich; eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist zu streichen.

10.2. Erweiterung und Präzisierung der Ausnahmen (Art. 14)

Die Ausnahmebestimmung von Art. 14 Abs. 3 lit. a VE-DSG ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur selten aus einem Gesetz. Häufiger sieht ein Gesetz zwingende Abklärungspflichten vor, welche mit Geheimhaltungspflichten verbunden sind und welche damit mit einer Einschränkung der Informationspflicht einhergehen. Die Bestimmung ist zu präzisieren und mit typischen Beispielen zu ergänzen (z.B. Abklärungen im Zusammenhang mit Geldwäscherei, Terrorismusbekämpfung und Korruption). Ausserdem können sich Verpflichtungen auch aus einem Vertrag ergeben. Eine weitere Ausnahme ergibt sich bei Datenbearbeitungen, die für eine Rechtsdurchsetzung erforderlich sind. Auch dies ist zu ergänzen.

Für die Einschränkung der Berufung auf überwiegende private Interessen, d.h. auf Fälle, in denen die Personendaten nicht Dritten bekannt gegeben werden, gibt es keine sachlichen Gründe. Besonders bei Konzernverhältnissen würde daraus ein enormer administrativer Mehraufwand resultieren. Sollte die betroffene Person durch die Bekanntgabe beeinträchtigt sein, so wäre dies im Rahmen der allgemeinen Interessensabwägung von Art. 24 VE-DSG zu berücksichtigen. Die Einschränkung ist damit zu streichen.

Die Bestimmung von Art. 14 Abs. 5 VE-DSG ist nicht praktikabel und zu streichen. Diese würde dazu führen, dass ständig einzelne Interessensabwägungen überprüft werden müssten. In grossen, komplexen Organisationen ist dies nicht zu bewerkstelligen.

10.3. Automatisierte Einzelfallentscheide (Art. 15)

Begrenzung des Anwendungsbereichs und der Pflichten; insb. keine Anhörungspflicht
Die Reichweite der neu eingeführten Informations- und Anhörungspflicht sowie Auskunftsrechte bei automatisierten Einzelfallentscheiden ist zu weitgehend. Zwar kennen die Konvention 108 und die EU eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE-DSG ist jedoch viel breiter: Der VE-DSG unterscheidet stärker zwischen Profiling und automatisierten Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden. Die Automatisierung ist ein zentraler Punkt der Digitalisierung und im heutigen wirtschaftlichen Umfeld von grundsätzlicher Bedeutung. Davon profitieren auch die Kunden, z.B. durch Objektivität der Entscheidung, schnellere Prozesse und damit besserer Nutzererfahrung sowie einer attraktiven Preisgestaltung.

Insbesondere das vorgesehene Äusserungsrecht der betroffenen Person bringt keinen Mehrwert; es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Die Offenlegung, wie bestimmte Entscheide zustande gekommen sind, betrifft zudem oft auch Geschäftsgeheimnisse.

Die Bestimmung ist entsprechend auf schwere Fälle, bzw. solche, die erhebliche Auswirkungen auf die betroffene Person haben, zu begrenzen. Der Wortlaut ist an die entsprechende Bestimmung in der EU-DSGVO anzupassen (insbesondere «Beeinträchtigung» statt «Wirkung» und «erhebliche» in Bezug auf beide Alternativen). Auch dann sind sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen sind. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung i.S.d. Gesetzessystematik ist ausreichend. Das Äusserungsrecht und der damit zusammenhängende Art. 20 Abs. 3 (Auskunftsrecht) sind zu streichen. Dies ist aufgrund des Derogationsrechts der Mitgliedstaaten der EU für die Äquivalenz nicht abträglich (vgl. Art. 22 Abs. 2 lit. c EU-DSGVO).

10.4. Datenschutz-Folgenabschätzung (Art. 16)

Beschränkung und Präzisierung / keine Pflicht des Auftragsdatenbearbeiters

Das in Art. 16 neu eingeführte Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) ist zu weit gefasst. Die offene und dadurch unklare Formulierung führt dazu, dass für praktisch alle Datenbearbeitungen vorgängig aufwändige Abklärungen durchgeführt werden müssten. Besonders problematisch ist die vorgesehene Sanktionierung bei Verstoss. Analog der EU-DSGVO ist eine Konkretisierung sowie Beschränkung auf Fälle vorzunehmen, bei denen ein «hohes Risiko» besteht. Darüber hinaus ist zu präzisieren, dass ein Risiko für eine Persönlichkeitsverletzung bestehen muss. Der Begriff «oder die Grundrechte» ist sodann zu streichen: Das Schweizer Recht kennt, anders als das europäische Recht, keine direkte Drittwirkung der Grundrechte. Schliesslich ist der Auftragsdatenbearbeiter von der Pflicht auszunehmen. Dieser verfügt regelmässig nicht über die notwendigen Angaben, sondern unterliegt den Entscheidungen des Verantwortlichen.

Streichung der Meldepflicht der Datenschutz-Folgeabschätzung

Die umfangreichen Meldepflichten sind ein unnötiger «Swiss Finish»: Sie sind unverhältnismässig und greifen in die Geheimsphäre der Unternehmen ein. Die zu erwartende «Meldeflut» ist für eine angemessene Reaktion des EDÖB kontraproduktiv. Problematisch ist auch die lange Frist, innert welcher der EDÖB Einwände mitteilen oder später eine Untersuchung einleiten kann. Damit werden falsche Anreize gesetzt. In der Gesamtheit bringt die Bestimmung keinen Mehrwert, führt jedoch zu erheblichen Rechtsunsicherheiten und innovationshemmenden Verzögerungen. Die Forderung der Konvention 108, bei geplanten Datenbearbeitungen Risiken einzuschätzen, wurde bereits durch Art. 11 VE-DSG (Datensicherheit) erfüllt. Schliesslich bestehen weitere Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen (z.B. im Bankengesetz). Doppelte Überwachungen sind aus Effizienzgründen zu vermeiden.

Die umfangreichen Meldepflichten bzw. Art. 16 Abs. 3 und folglich auch Art. 16 Abs. 4 VE-DSG sind zu streichen. Eine Meldung soll erst erfolgen, wenn eine Verletzung des Datenschutzes passiert ist, nicht bereits aufgrund von Risiken. Auch die Konvention 108 verlange nicht, die Behörden von der Datenschutz-Folgenabschätzung zu informieren. Eine Ausnahme der Meldepflicht sollte zumindest für Unternehmen mit einem betrieblichen Datenschutzbeauftragten vorgesehen werden.

10.5. Meldepflichten (Art. 17)

Beschränkung auf Verstösse mit gravierenden Folgen

Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse (inkl. Datenverluste) an den EDÖB (Data Breach Notification) ist stark einzuschränken. Sie erfasst weit mehr Fälle als die EU-DSGVO, welche diese Pflicht nur für Verletzungen von Sicherheitsmassnahmen vorsieht, die zusätzlich zu einem Bruch oder Verlust des Gewahrsams an den Daten führen. Zudem kann die vorgesehene Ausnahme sachlogisch nie angerufen werden, da eine «falsche» Datenbearbeitung per Definition immer eine Verletzung von Persönlichkeitsrechten ist.

Eine Pflicht ohne Eingrenzung in qualitativer und quantitativer Weise würde uferlos; jeder noch so geringe Verstoss müsste gemeldet werden, um den Sanktionsfolgen zu entgehen. Der Beauftragte sähe sich mit einer weiteren Meldungsflut konfrontiert und wäre ausser Stande, allfällig wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. Die Meldepflicht führt auch zu einem Konflikt mit dem strafrechtlichen Grundprinzip von «nemo tenetur» (vgl. Ziff. 14). Schliesslich wäre eine «unverzügliche» Meldung auch in zeitlicher Hinsicht nicht umsetzbar, da zuerst hinreichende Informationen gesammelt werden müssen. Zudem besteht die Gefahr, durch vorschnelles Handeln Geschäfts- oder Berufsgeheimnisse zu verletzen. So sieht die EU-DSGVO eine Frist von bis zu 72 Stunden vor.

Der Begriff des «Data Breach» sollte analog Konvention 108 und EU-DSGVO formuliert werden. Die Pflicht wäre damit auf Verstösse mit gravierenden Folgen zu beschränken, bei welchen ein Kontrollverlust an den Daten vorliegt. Als weiteres qualitatives Kriterium müsste die Tatsache ergänzt werden, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann. Dies z.B. mittels Unterstützung in Fällen, welche von den Verantwortlichen nicht mehr aus eigener Kraft bereinigt werden können. Weiter ist die Bestimmung durch ein quantitatives Element zu konkretisieren, z.B. auf Fälle, in welchen Daten von mindestens 100'000 Personen betroffen sind. Eine Meldung beim EDÖB muss den Schutz vor Sanktionen zur Folge haben (vgl. Ziff. 14.3).

10.6. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 18)

Anpassung der Reichweite und Überführung zu den Sicherheitsbestimmungen
Die Formulierung von Art. 18 VE-DSG geht ebenfalls über jene der EU-DSGVO hinaus. Zudem gehört diese systematisch zu Art. 11 VE-DSG (Sicherheit von Personendaten). Diese Bestimmung deckt die Anforderungen von «privacy by design» bereits. Art. 18 VE-DSG ist zu streichen, resp. in Art. 11 zu integrieren. Die Reichweite ist an das EU-Recht anzupassen.

10.7. Weitere Pflichten (Art. 19)

Verzeichnis statt allgemeine Dokumentationspflicht / Ausnahme für kleinere Unternehmen
Die allgemeine Dokumentationspflicht von Art. 19 lit. a VE-DSG ist bezüglich Inhalt und Umfang unklar und geht über die vergleichbare Bestimmung der EU hinaus. Die Pflicht ist analog der EU-DSGVO auf die Pflicht zur Erstellung «eines Verzeichnisses für regelmässige Datenbearbeitungen» einzuschränken. Die Pflicht, Datenschutzverstösse zu dokumentieren, ist zu weitgehend. Darüber hinaus ist auch eine Ausnahme der Pflicht für kleinere Unternehmen (z.B. analog EU mit weniger als 250 Mitarbeitenden oder am Umsatz gemessen) vorzusehen, sofern sie in Bezug auf den Datenschutz keine risikoreiche Tätigkeit ausüben. Aus systematischen Gründen sollte auch diese Bestimmung in Art. 11 VE-DSG integriert werden.

Beschränkung der Informationspflicht an Dritte
Die Reichweite der neu vorgesehenen Pflicht, Dritten die Berichtigung, Löschung oder Vernichtung von Daten zu melden, geht sehr weit und ist in der Praxis nicht umsetzbar. Eine solche Meldepflicht ist von Konvention 108 nicht und von der EU-DSGVO nicht in dieser Form vorgesehen. Die EU-DSGVO kennt eine entsprechende Meldepflicht nur unter gewissen Voraussetzungen im Zusammenhang mit dem «Recht auf Vergessen». Der VE-DSG erfasst demgegenüber auch unbedeutende Vorgänge; im täglichen Arbeitsprozess werden ständig Daten berichtigt, gelöscht oder vernichtet (z.B. weil ein Kunde bezahlt hat oder die Daten schlicht keine Relevanz

mehr haben). Die Auswirkungen dieser Meldepflicht wurden offenbar unterschätzt. Zu deren Bewältigung müsste eine neue Infrastruktur aufgebaut werden, welche sämtliche Empfänger über Jahrzehnte hinweg verwaltet. Eine betroffene Person ist besser in der Lage zu beurteilen, welche Daten für welche Empfänger (noch) von Interesse sind. Gerade solche Informationsansprüche der betroffenen Person sind aber bereits unter Art. 25 VE-DSG vorgesehen. Die Informationspflicht an Dritte ist analog der EU-DSGVO auf Fälle zu beschränken, in welchen die betroffene Person die Nachinformation aus berechtigten Gründen verlangt hat.

11. Auskunftsrecht (Art. 20)

Massnahmen gegen missbräuchliche Auskunftsbegehren
Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und hängige Verfahren bringt grosse Aufwendungen mit sich. Umso mehr, weil ein Auskunftsbegehren im Datenschutzsystem der Schweiz nie unverhältnismässig sein kann, da auch untergeordnete Datenschutzinteressen für einen Anspruch ausreichen. Gerade auch die vorgesehene umfassende Kostenlosigkeit des Auskunftsrechts führt zu Fehlanreizen: Es sind keine Massnahmen vorgesehen, welche es den Unternehmen erlauben würden, dem Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken Einhalt zu gebieten (vgl. Ziff. 3).

Es sind griffige Massnahmen gegen den Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken vorzusehen: Die Kostenlosigkeit ist zu relativieren, so z.B. bei unverhältnismässigem Aufwand und bei Ersuchen zu nicht ausschliesslich datenschutzrechtlichen Zwecken. Zudem sind weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. bei Art. 21 VE-DSG).

Einschränkung der Informationspflicht bei automatisierten Einzelfallentscheiden
Eine «Rechenschaftspflicht» in Bezug auf automatisierte Entscheide in der vorgesehenen detaillierten Form ist unverhältnismässig: Informationen darüber, wie bestimmte Entscheide zustande kommen, gehören zum Geschäftsgeheimnis. Durch die gewählte Formulierung wäre jedes Ergebnis, d.h. jeder Entscheid, erfasst. Dies würde zu einem zusätzlichen Administrativaufwand führen, ohne dass damit mehr Transparenz geschaffen würde. Im Gegenteil: Kunden würden Informationen erhalten, mit denen sie gar nichts anzufangen wissen (z.B. warum sie eine Werbeanzeige nicht erhalten haben).

Die geforderte Information über Vorliegen einer automatisierten Einzelfallentscheidung (Art. 20 Abs. 2 lit. e VE-DSG) sollte in allgemeiner Weise erfolgen. Die Bestimmung von Art. 20 Abs. 3 VE-DSG sollte in Art. 15 VE-DSG integriert werden. Dessen Grundsätze («erhebliche Auswirkung») wären dabei einzuhalten. Es muss klargestellt werden, dass das Auskunftsrecht nur von der jeweils tatsächlich betroffenen Person ausgeübt werden kann. Zudem ist ein Verweis auf die Einschränkungen des Auskunftsrechts bzw. der Informationspflichten (Art. 21 i.V.m. 14 VE-DSG) anzubringen.

12. Ausnahmetatbestände (Art. 21)

Ausweitung der Ausnahmen
Die vorgesehenen Ausnahmetatbestände gemäss Art. 14 VE-DSG sind zu eng formuliert und nicht konsistent. Die Informationspflicht sollte immer entfallen, wenn die Information nicht möglich oder unzumutbar ist. Eine Beschränkung auf Fälle der indirekten Beschaffung oder in denen keine Weitergabe an Dritte erfolgte, ist nicht nachvollziehbar. Die Bestimmung ist entsprechend anzupassen.

Es sind Ausnahmen, auch in Hinblick auf die rechtsmissbräuchliche Geltendmachung des Auskunftsrechts, für folgende bearbeiteten Daten vorzusehen:

- Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen;
- Aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption;
- Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden;
- Rein intern bearbeitete Daten;
- Daten über Drittpersonen;
- Unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.

Übergabe der Informationen an Dritte bei Missbrauchsverdacht (Neu)
Um Missbräuche zu verhindern, ist zudem vorzusehen, dass bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben werden können. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen. Eine Möglichkeit bestünde darin, dass der EDÖB den Entscheid über Herausgabe in Form einer anfechtbaren Verfügung vorlegt (vgl. analoge Regelung in Art. 8 Abs. 2 BPI).

13. Besondere Bestimmungen für die Datenbearbeitung durch private Personen (Art. 23, Art. 24)

Keine ausdrückliche Einwilligung beim Profiling (Art. 23)
Gemäss Art. 23 Abs. 2 lit. d VE-DSG gälte Profiling automatisch als Persönlichkeitsverletzung, wenn nicht vorgängig eine ausdrückliche Einwilligung eingeholt wird. Diese gesetzliche Vermutung stellt einen unbegründeten partiellen Paradigmenwechsel im Schweizer Datenschutzrecht dar (von grundsätzlicher Erlaubnis der Datenbearbeitung unter Einhaltung bestimmter Voraussetzungen zum Verbot mit Erlaubnisvorbehalt). Das Erfordernis der ausdrücklichen Einwilligung beim Profiling ist entsprechend zu streichen. Durch eine entsprechende Information kann genug Transparenz geschaffen werden. Eine Regelung hat unter Art. 15 VE-DSG zu erfolgen.

Klare und erweiterte Rechtfertigungsgründe (Art. 24)
Der Ausdruck «möglicherweise» in Art. 24 Abs. 2 VE-DSG schafft Rechtsunsicherheit. Die aktuelle Bestimmung (Art. 13 Abs. 2 DSG) wurde unnötigerweise geändert und sollte beibehalten werden.

Art. 24 Abs. 2 lit. a VE-DSG sollte analog Art. 6 Abs. 1 lit. b VE-DSG Verträge berücksichtigen, die zu Gunsten oder im Interesse der betroffenen Person geschlossen werden.

14. Aufsicht und Sanktionen (Art. 50 bis 55)

Das vorgeschlagene Sanktionsmodell stösst branchenübergreifend auf Kritik und ist aus Sicht der ICT-Wirtschaft nicht geeignet. Entsprechend wird zu diesem Kapitel umfassend Stellung genommen und es wird eine Grobskizze für einen alternativen Vorschlag für ein im Datenschutzgesetz zu integrierendes Sanktionsmodell.

14.1. Ausgangslage

Anders als der VE-DSG setzen die Konvention 108 und die EU-DSGVO in erster Linie auf Verwaltungssanktionen gegen Unternehmen. Bei der Regelung der Sanktionierung von Datenschutzverletzungen besteht gemäss den europäischen Bestimmungen ein erheblicher Spielraum: Die Konvention verlangt im Wesentlichen geeignete gerichtliche und nicht-gerichtliche Sanktionen und Rechtsmittel (Art. 10 E-SEV 108). Die EU-DSGVO und auch die Richtlinie 2016/680 sprechen von wirksamen, verhältnismässigen und abschreckenden Sanktionen. Es ist dabei den Mitgliedsstaaten überlassen, zu entscheiden, ob Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind (Erw. 149 und 152).

14.2. Kritik am Vorentwurf und weitere Überlegungen

Die im VE-DSG vorgesehenen Sanktionen und insbesondere der Weg über das Strafrecht sind nicht zielführend.

Persönliche Strafbarkeit der Mitarbeitenden
Die Mitarbeitenden eines Unternehmens geraten durch die persönliche Strafbarkeit zu stark in den Fokus der Sanktionen. Verschärft wird dies durch die Höhe der Bussen und die vorgesehene Möglichkeit, sogar fahrlässiges Handeln zu bestrafen. Damit wird der risikobasierte Ansatz, der mit der Revision verfolgt wird, untergraben.

Strafrechtliche Sanktionen führen dazu, dass Mitarbeitende in Zukunft selbständig jeden (möglichen) Verstoss bei den Behörden melden müssen. Dies birgt das Risiko, dass sie sich gegenseitig anzeigen, um nicht selbst ins Visier der Strafbehörde zu geraten. Der VE-DSG bietet zudem Dritten viele Anknüpfungspunkte (sobald eine Datenerhebung stattgefunden hat), um Anzeige zu erstatten. Dies kann zum Unterlaufen der intern definierten Datenschutz-Governance und zu Unruhen innerhalb der Unternehmen führen sowie entsprechende Reputationsschäden nach sich ziehen.

Verurteilte Mitarbeitende wären sowohl intern als auch extern stark exponiert. Es dürfte daher mittelfristig schwierig werden, qualifiziertes Personal zu finden, das bereit ist, die Verantwortung mit den einhergehenden Risiken zu tragen. Die Folge wäre ein sukzessives Abfallen der Qualität im Bereich der Datenbearbeitung.

Die persönliche Strafbarkeit der Mitarbeitenden entspricht auch nicht der von anderen Schweizer Gesetzen vorgesehen Linie (vgl. KG, UWG, FMG, BEHG), bei welchen der Fokus klar auf der Sanktionierung der Unternehmen liegt.

Die strafrechtliche Sanktionierung würde schliesslich insbesondere die KMU stark belasten. Bei übersichtlichen Verhältnissen ist die Identifikation fehlbarer Mitarbeitender relativ einfach; entsprechend bestünde ein Anreiz für die Strafverfolgungsbehörden, gerade bei solchen Unternehmen unverhältnismässig streng vorzugehen.

Verstoss gegen strafrechtliche Grundprinzipien
Problematisch sind die im VE-DSG vorgesehenen Mitwirkungspflichten angesichts des im Strafrecht vorherrschenden Grundsatzes des «nemo tenetur» bzw. des Selbstbelastungsverbotes. Die Pflicht, Datenschutzverstösse zu melden, käme faktisch einer Pflicht zur Selbstanzeige gleich. Der VE-DSG geht von einer verschuldensunabhängigen Sanktionierung aus und steht damit im Widerspruch zum Verschuldensprinzip: Bei Vorliegen des objektiven Tatbestandes wird direkt darauf geschlossen, dass auch der subjektive Tatbestand erfüllt ist. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind offen formuliert (vgl. Art. 16 Abs. 1 VE-DSG: «…vorgesehene Datenbearbeitung [führt] voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person»). Dies ist mit dem strafrechtlichen Bestimmtheitsgebot bzw. einer hinreichenden Voraussehbarkeit einer Strafbarkeit nicht vereinbar.

Umfang von potentiellen Verstössen und Meldungen
Datenbearbeitungen stellen innerhalb der Unternehmen eine alltägliche Aktivität dar. Unternehmen können im Zeitalter der Digitalisierung nicht mehr wählen, ob eine entsprechende Handlung vorzunehmen ist oder nicht. Damit unterscheidet sich das Datenschutzrecht beispielsweise vom Kartellrecht. Im VE-DSG sind kaum Erheblichkeitsschwellen vorgesehen. Folglich würde jede geringfügige Unregelmässigkeit in alltäglichen Datenbearbeitungsvorgängen eine Datenschutzverletzung darstellen. Die daraus resultierende Mitteilungsmenge an den Beauftragten sowie die drastischen Sanktionsfolgen wären höchst problematisch.

Strafkatalog
Im Kern entspricht der Strafkatalog grundsätzlich den europäischen Bestimmungen. Hingegen werden die Berufspflichten erheblich verschärft und es wird sogar eine Freiheitsstrafe als Sanktion vorgesehen. Diese Ausweitung des Berufsgeheimnisses ist als überschiessende Bestimmung klar abzulehnen; es können in dieser Hinsicht nicht alle Berufe mit jenen von Art. 321 StGB gleichgesetzt werden.

Fazit
Die strafrechtlichen Sanktionen des VE-DSG, die gegen Mitarbeiter eines Unternehmens ausgesprochen werden können, sind weder verhältnismässig noch zielführend. Diese stehen im Widerspruch zu einer Vielzahl von schweizerischen strafprozessualen Prinzipen. Die auf Risikoausgleich ausgerichteten Möglichkeiten des VE-DSG werden damit ausgehöhlt und der Interessensausgleich wird unnötig eingeschränkt. Gesamthaft geht das vorgeschlagene strafrechtliche Sanktionsmodell damit deutlich über die im europäischen Raum vorgesehenen Sanktionen, die in erster Linie verwaltungsrechtlicher Natur sind, hinaus.

14.3. Vorschlag der Wirtschaft für ein Sanktionsmodell im DSG

Aufgrund der vorangehenden Überlegungen sprechen wir uns für ein alternatives Sanktionsmodell aus. Nicht strafrechtliche Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen sollen dabei im Vordergrund stehen.

Auch bei Verwaltungsstrafen ergeben sich verschiedene Problemfelder, gerade auch aus rechtsstaatlicher Sicht. Das nachfolgend skizzierte Modell berücksichtigt diese und schlägt ein auf die spezielle Konstellation des Datenschutzes angepasstes, verwaltungsrechtliches Sanktionsmodell vor. Dieses soll effizient ausgestaltet sein, die richtigen Anreize setzen und den Anforderungen an ein faires Verfahren entsprechen.

Grundsatz: verwaltungsrechtliche Sanktionen gegen Unternehmen
Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen. Anknüpfungspunkt sind dabei Organisationsmängel im Unternehmen. Lediglich subsidiär soll eine strafrechtliche Verfolgung von Mitarbeitenden möglich sein. Anzeigen sollen in der Regel durch die Unternehmen selbst erstattet werden. Im Ergebnis würde eine Anpassung des Sanktionsziels die Situation für die Datenbearbeitenden im Sinne einer Verbesserung des Datenschutzes im Unternehmen massgeblich entschärfen.

Weiter soll eine Sanktionierung der Mitarbeitenden nur bei direkt vorsätzlichem Handeln, das sich gegen die Interessen des Unternehmens und/oder der betroffenen Person richtet, in Frage kommen. In diesem Zusammenhang ist eine Abstimmung mit den bereits im BT StGB vorgesehenen Strafbestimmungen erforderlich. Diese dürften für die Bestrafung der natürlichen Person meist schon ausreichen (z.B. Verletzung des Geschäftsgeheimnisses und unbefugte Datenbeschaffung). Der Kreis der potentiell strafrechtlich verantwortlichen Mitarbeitenden müsste zum Vornherein eingeschränkt werden (entsprechend Art. 29 StGB).

Angepasste Rolle des EDÖB und verbesserte Gewaltentrennung durch eine neu zu bildende Spruch-Behörde
Eine Behörde, die gleichzeitig über Untersuchungs- und Spruchkompetenzen verfügt (wie bei Sanktionen mit verwaltungsrechtlichem Charakter üblich), hat die Tendenz, eine mit dem Prinzip der Gewaltenteilung nur schwer vereinbare Machtfülle zu erlangen. Die Verwaltungssanktionen sollten daher nicht von der Untersuchungsbehörde verhängt werden.

Die Ausstattung des EDÖB mit Spruchkompetenzen, sogar die im VE-DSG bereits vorgesehene Ausstattung mit Verfügungskompetenzen, kann dazu führen, dass der EDÖB zu mächtig wird. Zusätzlich besteht die Gefahr, dass eine vertrauensvolle Zusammenarbeit mit den Unternehmen im Bereich der wichtigen Beratung beeinträchtigt wird. Ein auf Vertrauen basierender Austausch mit den Unternehmen ist für die Tätigkeit des Beauftragten jedoch von grundsätzlicher Bedeutung, dies umso mehr, als ihm gemäss VE-DSG die Aufgabe zukommt, Empfehlungen der guten Praxis zu erlassen.

Die Verfügungskompetenzen sowie die Sanktionskompetenz könnten entsprechend in einer neu zu bildenden «Datenschutz-Kommission» gebündelt werden. Diese könnte beispielsweise dem EDI oder EJPD angehängt sein. Ausschliesslich dieser kämen nebst der Sanktionskompetenz auch die Verfügungskompetenzen zu, dies

gerade auch im Bereich vorsorglicher Massnahmen. Das Verhältnis zwischen «Datenschutz-Kommission» und EDÖB müsste präzisiert werden, insbesondere in Bezug auf die Überwachungs- und Untersuchungskompetenzen des Beauftragten i.S.v. Art. 40 f. VE-DSG.

In dieser Struktur würde der EDÖB seine bisherigen Aufgaben wahrnehmen und eine Vorselektion der ihm zugetragenen Fälle machen. Sollte sich in einem Fall eine mögliche Strafbarkeit abzeichnen, würde er die Angelegenheit der «Datenschutz-Kommission» weiterleiten. Bei Verfahren auf dieser zweiten Stufe würde die verwaltungsrechtliche Mitwirkungspflicht des Beauftragten wegfallen. Gegen Entscheide dieser Spruchbehörde stünde den Betroffenen der Weg zum Bundesverwaltungsgericht als Rechtsmittelinstanz offen.

Strafkatalog

Der Strafkatalog ist mit jenem der EU-DSGVO abzugleichen, soll jedoch nicht darüber hinausgehen. Folgende Anpassungen sind erforderlich:

- Konkretisierung / Streichung der zu offen formulierten Tatbestände;
- Beschränkungen und Anpassungen bei den Pflichten des Verantwortlichen und Auftragsbearbeiter sind beim Strafkatalog zu berücksichtigen;
- Fokus auf wesentliche Bedrohung für die Privatsphäre der betroffenen Person;
- Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens in Bezug auf die betroffene Person orientiert. Zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung vorsätzlich vorgenommen wurde;
- Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten;
- Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab 2. Stufe des Verfahrens (siehe unten);
- Beschränkung der beruflichen Schweigepflicht auf Fälle, in denen die betroffene Person eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages).

Mitwirkungspflichten und Strafmilderungsgründe

Neben der im Vorentwurf vorgesehenen Pflicht, Datenschutzverstösse bei den Behörden zu melden, besteht für die Unternehmen im verwaltungsrechtlichen Verfahren generell eine Mitwirkungspflicht. Wie oben kritisiert, läuft die Idee der anschliessenden Bestrafung im Rahmen eines Strafverfahrens diesem Konzept entgegen und verstösst zusätzlich gegen das Selbstbelastungsverbot. Ein kooperatives Verhalten, das letztlich einer raschen Schadensminderung dienen soll, muss gefördert werden. Unternehmen, die den Beauftragten über eine Verletzung der Datenschutzbestimmungen informieren, mit den Behörden kooperieren, Fehler aktiv korrigieren und grössere Risiken zu verhindern suchen, sollen mit einer Reduktion der Sanktion oder gar dem Absehen von einer Sanktion rechnen können (vgl. auch Art. 49a Abs. 2 KG). Dieser auf Schadensminderung ausgerichtete Ansatz entspricht den modernen Grundsätzen der Corporate Governance und fördert gleichzeitig das Ziel, ein hohes Datenschutzniveau zu erreichen.

Gründe, die strafmildernd wirken sollten, wären:

- Compliance-Defense: Implementierung eines tauglichen Compliance-Programmes;

- Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Richtlinien, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden;
- Handeln nach Treu & Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (z.B. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art»;
- Wahrung berechtigter Interessen: Güterabwägung im Fall von Pflichtenkollision mit anderen zwingenden Rechtsregeln (z.B. unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse zur Abwendung eines Unternehmenskonkurses; vgl. Notstand, Art. 17 StGB);
- Rechts- und Sachverhaltsirrtum (vgl. Art. 13 und 21 StGB);
- Strafrechtliche Verfolgung eines Mitarbeitenden. Eine Anzeige gegen einen direktvorsätzlich handelnden Mitarbeitenden durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden;
- Aktive Schadensverminderung und Zusammenarbeit mit den Behörden.

Sanktionen

Datenbearbeitungen gehören zur täglichen Arbeit der Unternehmen. Datenschutzverletzungen können dementsprechend im Rahmen des Tagesgeschäftes geschehen. Dies muss bei der Festlegung der Sanktionshöhe einen Einfluss haben. Hierbei sind die gesamten Umstände des Einzelfalles zu berücksichtigen, so z.B. die Schwere und die Auswirkungen des Verstosses sowie die oben genannten Strafmilderungsgründe. Ebenso muss, in Anlehnung an die EU-DSGVO, eine Konkurrenzklausel eingefügt werden: Bei gleichen oder miteinander verbundenen Datenbearbeitungsvorgängen, durch die vorsätzlich mehrere Bestimmungen des VE-DSG verletzt wurden, darf der Gesamtbetrag der Busse nicht denjenigen Betrag übersteigen, der für die schwerwiegendste Verletzung vorgesehen ist.

15. Übergangsfristen (Schlussbestimmungen, Abs. 10)

Im VE-DSG fehlt eine umfassende Übergangsregelung. Die neuen und revidierten Bestimmungen werden die Prozesse der Unternehmen bedeutend beeinflussen. Es ist deshalb eine allgemeingültige Übergangsbestimmung von zwei Jahren aufzunehmen. Von einer Rückwirkung ist abzusehen.

16. Zusammenfassung der Kernanliegen

Die Schweizer Datenpolitik und damit auch die Datenschutzregulierung sollte sich an den übergeordneten Zielen der Strategie «Digitale Schweiz» des Bundesrates orientieren: Zu berücksichtigen ist insbesondere der Nutzen der Daten für den digitalen Fortschritt und die Ausschöpfung des wirtschaftlichen Potentials im Interesse der Konsumenten und Unternehmen. Eine einseitige Orientierung an potentiellen Risiken wäre verfehlt. Im Grundsatz sind Behinderungen von Innovation und Entwicklungen durch Datenschutzvorgaben zu vermeiden.

Im Datenschutzgesetz ist für die Schweizer Unternehmen ein Maximum an Flexibilität und ein Minimum an Belastung zu wahren. Spielräume im Verhältnis zum internationalen Recht und das etablierte System der Selbstregulierung sind so weit als möglich zu nutzen. Die im Vergleich zum EU-Raum überschiessenden Regelungen sind anzupassen. Dabei soll die Totalrevision auch genutzt werden, um bestehende Bestimmungen zu hinterfragen und an die technologische Entwicklung anzupassen.

Zusammenfassend lassen sich in Bezug auf die VE-DSG folgende vier Hauptforderungen festhalten:

- Diverse **Informations- und Meldepflichten** gehen zu weit. Sie bedeuten unverhältnismässigen Aufwand und generieren eine regelrechte «Flut» an Informationen und Meldungen. Abzulehnen sind auch die damit verbundene Offenlegung von Geschäftsgeheimnissen und die Pflicht, sich selbst zu belasten. Gesamthaft wirken sich die vorgeschlagenen Pflichten innovations- und wettbewerbshindernd aus. Sie sind dem vom Vorentwurf angestrebten risikobasierten Ansatz entsprechend substantiell zu reduzieren. Dies betrifft insbesondere automatisierte Einzelfallentscheide, Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzverstössen. Darüber hinaus braucht es eine Relativierung der Kostenlosigkeit des Auskunftsrechts und weitere, griffige Massnahmen, um dem Missbrauch des Datenschutzrechtes zu datenschutzfremden Zwecken entgegenzuwirken.
- Ein weiterer umfassender Kritikpunkt ist das vorgeschlagene **Sanktionssystem**: Private, strafrechtliche Sanktionen sind weder verhältnismässig noch zielführend. Es ist ein tragbares, mit den rechtsstaatlichen Grundsätzen vereinbares Sanktionssystem zu implementieren. Gleichzeitig ist eine zu grosse Machtfülle des EDÖB zu verhindern.
- Der Begriff «**Profiling**» ist auf automatisierte Bewertungen von Personendaten einzuschränken und die Bedingungen dazu sind stark zu reduzieren (Information statt Einwilligung).
- Die Initiative für Empfehlungen der guten Praxis muss zwingend von (Branchen-)Verbänden ausgehen. Die **Selbstregulierung** ermöglicht es mittels Bezug zur Praxis, sachgerechte Lösungen zu entwickeln. Der betriebliche Datenschutzbeauftragte ist auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen.

Wir danken Ihnen für die Aufmerksamkeit, die Sie unseren Anliegen entgegenbringen.

Freundliche Grüsse

Andreas Kaelin
Geschäftsführer ICTswitzerland

Amstutz Jonas BJ

Von: ERARD Frédéric <frederic.erard@unine.ch>
Gesendet: Dienstag, 4. April 2017 11:11
An: Amstutz Jonas BJ
Cc: SPRUMONT Dominique
Betreff: Prise de position révision LPD - IDS
Anlagen: Révision LPD_prise de position IDS.docx.doc

Cher Monsieur,

Je vous prie de trouver ci-joint la prise de position de l'Institut de droit de la santé (IDS) de l'Université de Neuchâtel sur l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données.

Je vous prie de croire, cher Monsieur, à l'expression de mes sentiments les meilleurs,

Frédéric Erard
Assistant doctorant
Institut de droit de la santé
Faculté de droit
Université de Neuchâtel
Avenue du 1er-Mars 26
CH-2000 Neuchâtel
Tél. +41 32 718 12 77

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avis donné par

Nom / société / organisation : Institut de droit de la santé, Université de Neuchâtel

Abréviation de la société / de l'organisation : IDS

Adresse : Av. du 1er-Mars 26, 2000 Neuchâtel

Personne de référence : Prof. Dominique Sprumont, Frédéric Erard

Téléphone : 032 718 12 80

Courriel : dominique.sprumont@unine.ch

Date : 4 avril 2017

Remarques importantes :

1. Nous vous prions de ne pas modifier le formatage de ce formulaire !
2. Utilisez une ligne par article, alinéa et lettre ou par chapitre du rapport explicatif.
3. Veuillez faire parvenir votre avis au **format Word** d'ici au 4 avril 2017 à l'adresse suivante : jonas.amstutz@bj.admin.ch

Nous vous remercions de votre collaboration!

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Table des matières

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Remarques générales

nom/société	remarque / suggestion :
IDS	L'IDS salue la volonté de réviser la loi fédérale sur la protection des données. Celle-ci est devenue non seulement nécessaire en raison du développement du droit international et européen, mais également en raison du développement des nouvelles technologies de l'information et de la communication. Il est par conséquent essentiel d'adapter le cadre légal applicable aux contraintes actuelles et futures.
IDS	De manière générale, l'avant-projet de révision de la LPD est a été judicieusement conçu. L'IDS émet toutefois des réserves, en particulier en lien avec la protection des données relatives à la santé. Les données personnelles relatives à la santé constituent une catégorie de données particulièrement sensibles en tant qu'elles permettent, directement ou indirectement, de tirer des conclusions sur l'état de santé, physique, mental ou psychique d'une personne (MEIER, Protection des données, Berne 2011, N 486). Avec l'évolution de la science, les données collectées en lien avec la santé sont devenues de plus en plus pointues et intimes (ex. : encodage génétique). Par ailleurs, les méthodes de collecte et de stockage développées permettent aujourd'hui de traiter un nombre très élevé de données concernant la santé des individus. Accumulées, ces données peuvent être utilisées à de multiples fins (assurances, recherche scientifique, réseaux sociaux, habitudes de consommation, etc.) qui présentent un haut potentiel de nuisance pour les individus. Si les collectes de données sur la santé peuvent présenter des avantages pour la société (ex. : résultats de recherche bénéfiques), elles présentent aussi des risques de préjudices graves à l'égard des personnes dont les données sont collectées. Ainsi, le traitement illicite de données génétiques à des fins malveillantes est susceptible de mettre au ban de la société les personnes concernées. De tels agissements peuvent avoir des conséquences graves sur la vie des personnes concernées, en particulier du point de vue des assurances, du travail ou de la vie privée. Au regard de la nature et du nombre de données relatives à la santé qui sont aujourd'hui collectées, ainsi que des risques encourus par un traitement illicite de ces données, il est primordial d'encadrer strictement le traitement des données personnelles relatives à la santé. De ce point de vue, l'avant-projet de révision de la LPD devrait mieux prendre en compte les risques liés à cette thématique.
IDS	Le concept d'anonymisation des données doit être appréhendé de manière très prudente, en particulier en matière de données personnelles relatives à la santé. Avec le développement des techniques génétiques, il est actuellement aisé de relier un échantillon biologique à un individu. En d'autres termes, il n'est plus possible d'anonymiser des données génétiques. Ce qui est vrai pour le domaine génétique l'est par ailleurs de plus en plus pour les données physiologiques d'un patient. Grâce au développement des techniques d'analyse des données physiologiques, il est

	maintenant fréquemment possible de rattacher des données physiologiques à un patient. Ce constat appelle l'adoption de règles particulièrement protectrices en matière de traitement de données relatives à la santé et une prudence toute particulière lorsqu'il est fait recours à l'anonymisation. Par ailleurs, l'utilisation des *big data* remet sérieusement en cause le principe même d'anonymisation puisque ces techniques permettent, par recoupement, d'identifier un grand nombre d'individus sur la base d'informations banales et a priori anonymes (ex. : code postal, sexe, etc.).
IDS	A l'heure actuelle, les échantillons biologiques humains font en partie l'objet d'un vide juridique. Dans la mesure où ceux-ci ne font pas l'objet d'une recherche au sens de la LRH, leur traitement n'est pas réglé par la loi. Or, en pratique, les collectes et la conservation d'échantillons humains ne sont pas forcément réalisées dans un objectif de recherche, ou alors le sont sans objectif prédéterminé (différents types de biobanques). Inclure les échantillons biologiques dans le champ d'application de la LPD renforce la proposition de traiter à part les données de santé sous l'angle de la protection des données. La révision de la LPD pourrait être l'occasion de combler ce vide juridique. Cela pourrait se traduire par une extension du champ d'application de la LPD aux échantillons biologiques dont la collecte et la conservation permettraient de tirer des données personnelles. Une telle extension permettrait de garantir une protection minimale en attendant l'adoption d'une loi fédérale sur les biobanques (cf. motion Rebecca Ruiz du 17 mars 2017).
IDS	En ce qui concerne le champ d'application territorial de la LPD, le Tribunal fédéral a admis une application assez large de la LPD pour des traitements illicites de données collectées en Suisse, commis depuis l'étranger. La révision de la LPD offre une occasion particulièrement propice d'inscrire clairement dans la loi que tout traitement illicite de données collectées en Suisse, même commis depuis l'étranger, est soumis à la LPD et peut être condamné en Suisse en application de cette loi. Cette proposition est d'autant plus importante que la question du *big data* demeure traitée de manière trop vague.
IDS	Du point de vue des sanctions, il est regrettable que l'avant-projet n'octroie pas au PFPDT un véritable pouvoir de punir les contrevenants à la LPD au moyen d'amendes administratives, à l'instar de ce que prévoit le Règlement UE 2016/679. Privilégier les sanctions pénales, comme le fait l'avant-projet, présente des inconvénients de taille. En effet, les sanctions pénales visent prioritairement les personnes physiques au sein des entreprises privées plutôt que les personnes morales elles-mêmes. Cela ouvre le champ à une impunité malvenue des entreprises qui traiteraient des données personnelles de manière illicite. Face à des entreprises aux capitaux importants, dont le modèle d'affaires repose principalement sur les collectes de données (géants du net, réseaux sociaux, société spécialisée dans la médecine personnalisée ou le *big data*, etc.), il est primordial de se doter d'un cadre légal fort, assorti de sanctions importantes et dissuasives. Ainsi, il est nécessaire de doter le PFPDT d'un pouvoir de condamner les contrevenants à des amendes administratives d'un montant dans l'ordre de grandeur de ce que prévoit l'article 83 du Règlement (UE) 2016/679, à savoir des amendes administratives pouvant s'élever jusqu'à 20 millions d'euros, ou

	dans le cas d'entreprise, jusqu'à 4% du chiffre d'affaires mondial total de l'exercice précédent si ce montant dépasse 20 millions d'euros. En l'absence de sanctions administratives fortes, la Suisse pourrait rapidement devenir un paradis pour les sociétés souhaitant être soumises à des réglementations légères, avec le risque que les pays voisins de la Suisse considèrent que cette dernière ne bénéficie plus d'un niveau adéquat de protection.
IDS	La problématique du *big data* a probablement été sous-estimée dans l'avant-projet de révision de la LPD. Alors que le *big data* pose des questions nouvelles, l'avant-projet ne semble connaître aucune évolution majeure sur ce point, malgré les objectifs affichés dans le rapport explicatif. Dans les grandes lignes, l'avant-projet se contente en effet d'assimiler les activités liées au *big data* au profilage. Ce faisant, il n'apporte malheureusement pas de règles spécifiques à l'appréhension du *big data*. L'adoption de règles spécifiques dans ce domaine paraît pourtant judicieuse, car les principes généraux de la LPD ne semblent plus adéquats pour répondre aux défis posés par le *big data*. Par exemple, dans le contexte du *big data*, les collectes de données sont souvent menées sans que la finalité du traitement ne soit nécessairement connue. Cela pose des problèmes sérieux du point de vue du consentement des personnes concernées, dans la mesure où il n'est alors pas possible de leur offrir une information précise sur le but du traitement. Par ailleurs, toujours dans ce contexte, l'utilisation de données *a priori* anonymes (et donc non soumises à la LPD) permettent fréquemment, par recoupement, de procéder à l'identification d'une personne. Face à ce phénomène, il paraît donc judicieux de requestionner la notion même de données personnelles et d'examiner si le champ d'application matériel de la LPD ne devrait pas être redéfini. Parmi d'autres problématiques, le principe d'exactitude est également mis à mal avec l'utilisation des *big data*. Dans ce contexte, on fait en effet usage d'algorithmes pour identifier des corrélations de données. Les résultats aboutissent à des informations/données nouvelles liées à des personnes, qu'il n'est pas possible de vérifier dans la mesure où elles sont le résultat de probabilités ou d'interprétations (pour plus de détails sur les problématiques mentionnées ci-dessus, voir notamment : FANTI S., *Big data & protection des données dans le domaine de la santé*, in : SPRUMONT D. (édit.), Nouvelles technologies et santé publique, 22ème Journée de droit de la sa santé, Berne 2016 ; JACCARD M.*, De la protection des données à la sécurisation des données connectées ?*, in : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20ème « Marathon du droit », Genève 2015, p. 491 ss.) L'environnement des *big data* évolue rapidement et il est capital d'appréhender juridiquement ce phénomène avant qu'il ne s'impose « de fait ». En raison des dangers potentiels qui entourent une utilisation malveillante des *big data*, la révision de la LPD constitue une occasion qui doit être saisie pour mener une réflexion large sur cette question et adopter des règles adaptées aux contraintes nouvelles auxquelles nous devons aujourd'hui faire face. Il convient de ne plus attendre pour aborder la question.
IDS	On peut se demander si la LPD doit offrir une protection particulière aux données personnelles relatives à la santé ou si cette protection n'est pas déjà offerte par un certain nombre de lois spéciales. En effet, la future loi fédérale sur le dossier électronique sur le patient ou la future loi fédérale

	sur l'enregistrement des maladies oncologiques offrent des garanties de protection particulières aux données médicales. Par ailleurs, les données médicales sont protégées par le dispositions relatives au secret médical (not. : art. 321 et 320 CP, différentes lois fédérales sur les professions médicales, lois cantonales sur la santé) ou au secret de la recherche. Malgré le cadre légal existant, il est selon nous primordial que la LPD assure des garanties spécifiques de protection aux données personnelles relatives à la santé. En effet, les données relatives à la santé ne sont plus seulement collectées par des soignants, mais par un grand nombre de sociétés susceptibles de les utiliser à des fins commerciales (géants du net, assurances, etc.) par le biais des réseaux sociaux ou d'objet connectés notamment. Or, ces acteurs ne sont pas soumis aux dispositions sur le secret médical et collectent les données médicales d'individus sur la base d'un consentement souvent discutable. Par ailleurs, les risques encourus aujourd'hui par une utilisation illicite de données de la santé est susceptible de déboucher sur des préjudices toujours plus graves. Il est primordial que les personnes dont les données personnelles relatives à la santé sont collectées puissent garder un contrôle sur ces données. Or, à l'exception de la LPD, aucune loi fédérale ne protège ce type de données en tout type de situations. La loi fédérale sur le dossier électronique du patient (LPEP) ne s'applique en effet qu'aux communautés certifiées et seulement si le patient a souhaité constituer un dossier électronique. Par ailleurs, les règles applicables en matière de secret médical se bornent en grande majorité à punir la violation du secret, mais ne règlent pas les modalités de traitement des données médicales. La loi laisse ainsi subsister des lacunes importantes en matière de protection des données de la santé. En l'absence d'une loi fédérale sur la santé, cette question devrait être réglée de manière spécifique dans la LPD. La révision de la LPD devrait ainsi être saisie pour intégrer des considérations relatives à cette question. Il conviendrait dans ce sens d'évaluer la possibilité d'identifier les données de santé comme une catégorie à part dans la LPD au même niveau que les données sensibles. Cela permettrait de fixer le cas échéant un régime particulier pour ces données de santé qui tiennent compte des nombreuses lois spéciales en la matière (LDEP, LRMO, LAGH, LRH, etc).
IDS	Dans le cadre de la présente prise de position, l'absence de remarque sur une disposition ne vaut pas approbation de la part de l'IDS.

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

nom/société	loi	art.	al.	let.	remarque / suggestion :
IDS	LPD	2			Dans sa jurisprudence « Google Street View » (ATF 138 II 346, c. 3), le Tribunal fédéral a appliqué la

					théorie des effets. Il a ainsi considéré la prise d'images en Suisse et la publication de celles-ci de façon à pouvoir être utilisées en Suisse créaient un point de rattachement prépondérant avec la Suisse, mêmes lorsque ces images étaient traitées depuis l'étranger. Dans ce cas, le Tribunal fédéral a reconnu l'application de la LPD ainsi que la compétence du Préposé fédéral à la protection des données (PFPDT). L'occasion devrait être saisie ici de codifier clairement cette pratique et de la renforcer. Il serait ainsi bienvenu de soumettre le traitement de toutes les données collectées en Suisse à la LPD et au pouvoir de contrôle du PFPDT. Une telle réglementation permettrait d'éviter les hésitations relatives au critère du « rattachement prépondérant » et encouragerait les collecteurs de données étrangers à agir en conformité avec la LPD. Nous proposons la modification suivante de l'article 2 al. 1 LPD : « *La présente loi régit le traitement de données concernant des personnes physiques,* ***collectées en Suisse ou à partir de la Suisse****, effectué par : (…)* » Nous proposons par ailleurs d'étendre le champ d'application de la loi aux échantillons biologiques, dans la mesure où ils sont collectés et conservés de telle sorte qu'il est possible d'en tirer des données personnelles. Un alinéa 1bis pourrait être ajouté avec la teneur suivante : « *[1bis] Elle régit également la collecte et la conservation de matériel biologique humain dans la mesure où il est possible d'en tirer des données personnelles. Sont réservées les dispositions de la loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain.* »
IDS	LPD	5			Le transfert de la compétence de déterminer si une législation assure un niveau protection adéquat en faveur du Conseil fédéral (et non plus au maître du fichier) est à saluer.
IDS	LPD	7	2		Lorsqu'il s'agit de données personnelles relatives à la santé, la sous-traitance de données présente des risques accrus. Il est donc primordial que la sous-traitance de telles données, qu'il s'agisse des données sur la santé ou de l'ensemble des données sensibles, soient soumises à des conditions

					précises, inscrites directement dans la LPD. La solution proposée à l'article 7 al. 2 AP-LPD est trop imprécise. En outre, en raison de la nature particulière de données relatives à la santé, les personnes qui sous-traitent des données relatives à la santé devraient être soumises à des exigences particulières de contrôle. Il serait par exemple judicieux de soumettre ces personnes à l'obtention d'une certification spécifique (au sens de l'article 10 AP-LDP). Le champ d'application de cette disposition dépasserait le cadre du champ d'application de loi fédérale sur le dossier électronique du patient et contribuerait à favoriser la sécurité de données de la santé.
IDS	LPD	10			Il est indispensable que les organismes suisses ou étrangers qui traitent à grande échelle des données sur la santé collectées en Suisse soient soumis à une forme de contrôle. La certification obligatoire semble être l'instrument le plus adapté pour assurer ce contrôle. Elle permet en effet d'assurer que toutes les personnes soumises à la certification, suisses ou étrangères, prennent connaissance et respectent les dispositions réglementaires applicables au traitement de données de santé, en particulier lors de la collecte de telles données. Le cercle des personnes ou institutions soumises à l'exigence de certification obligatoire devrait toutefois être soigneusement déterminé. Il faudrait en effet éviter de soumettre les cabinets médicaux ou les hôpitaux à l'exigence de certification. Il serait également judicieux d'exempter d'une telle obligation les personnes privées ou organes fédéraux qui sont amenées, de par la loi, à traiter des données sur la santé. Nous visons notamment ici les assurances maladies. Toutes les autres personnes ou institutions, à l'instar des entreprises qui collectent des informations sur la santé de personnes ou autres hébergeurs de données sur la santé, seraient soumises à une obligation de certification. Nous proposons ainsi l'ajout d'un article 10 al. 1bis dont la teneur pourrait être la suivante : « *[1bis] Le traitement de données sur la santé est soumis à une certification obligatoire. Sont exemptés d'une telle certification :* *a. les professionnels de la santé au bénéfice d'une autorisation de pratique à titre indépendant;*

					b. les institutions de santé au bénéfice d'une autorisation d'exploitation ; *c. les organisations qui, de par la loi, sont amenées à traiter des données sur la santé.* »
IDS	LPD	12			L'article 12 AP-LPD n'est pas acceptable. Les données médicales sont protégées par les dispositions relatives au secret professionnel (art. 321 CP, lois cantonales sur la santé), au secret de fonction (art. 320 CP) et aux devoirs professionnels des soignants (art. 40 LPMéd, 27 LPsy et 16 future LPSan). Le secret professionnel poursuit plusieurs intérêts, en particulier : - La protection de la sphère intime et privée du patient, qui doit pouvoir se fier entièrement à la discrétion du professionnel en vue de lui livrer toutes les informations qui lui permettront de recevoir le traitement le plus adapté. - L'intérêt de l'Etat à ce que les professions médicales puissent être exercées correctement et sans entrave, dans la mesure où ces professions ne peuvent être exercées que si elles inspirent au public une confiance suffisante, moyennant de sérieuses garanties de discrétion. - L'intérêt du professionnel de la santé à ce qu'un rapport de confiance existe avec son patient, de manière à pouvoir exercer son métier efficacement. - La protection des informations qui concernent des tiers et qui auraient été divulguées dans le cadre de la relation thérapeutique. Selon la jurisprudence, le secret médical continue de déployer ses effets après la mort du patient (ATF 87 IV 105). Même si la personnalité finit par la mort (art. 31 CC), il n'apparaît pas dépourvu de sens de garantir aux justiciables qu'après leur décès, les renseignements figurant dans leur dossier médical demeureront couverts par le secret médical et ne seront divulgués *sans un contrôle sévère* (arrêt du Tribunal fédéral du 3 novembre 1989, RDAF 1990 p. 45, c. 4b). L'article 12 AP-LPD ouvre une brèche inacceptable au maintien du secret médical après la mort du patient. Si le défunt n'a pas de son vivant interdit expressément la consultation de son dossier après sa mort, cette disposition permettrait en effet à tout tiers présentant un intérêt légitime de consulter son

					dossier si aucun intérêt prépondérant du défunt ou d'un tiers l'en empêche. Sous l'angle de la pratique médicale, cette disposition est problématique à plusieurs titres : - L'article 12 AP-LPD supprime au responsable du traitement le droit d'invoquer le secret professionnel ou de fonction. De ce fait, il remet en cause l'existence même du secret médical après la mort du patient. Cela est propre à entamer la confiance nécessaire que le public doit placer dans les professions médicales afin de garantir le bon exercice de ces dernières. Le secret professionnel, le cas échéant de fonction, doit être maintenu après la mort du patient. - Le dossier médical d'une personne décédée peut contenir des données très sensibles que le défunt ne souhaitait pas divulguer aux membres de sa famille, même après sa mort. Les données médicales nécessitent une protection particulière, que l'article 12 AP-LPD n'assure pas suffisamment. - L'article 12 AP-LPD présume l'existence d'un intérêt légitime en faveur des personnes en lien de parenté directe avec le défunt ou mariées, en partenariat enregistré ou en concubinage. Or, le secret médical vaut précisément à l'égard de ces proches et il doit être maintenu par principe après la mort du patient. L'accès aux données médicales par les proches après la mort du patient est rendu ici trop aisé. L'assurance que les informations confiées par le patient ne seront jamais (avant ou après sa mort) transmises aux proches contribue directement à instaurer la confiance nécessaire au bon déroulement de la relation thérapeutique. - Selon l'article 12 AP-LPD, il revient au responsable du traitement (en matière médicale, au soignant) de procéder à l'examen de la demande de consultation et d'examiner s'il existe un intérêt légitime à la consultation. Au regard des intérêts en jeu, une telle prise de décision nécessiterait une analyse consciencieuse de tous les intérêts en cause et la vérification des motivations des tiers souhaitant consulter le dossier médical. Imposer cet exercice aux soignants créerait de nouvelles responsabilités à la charge de ces derniers et constituerait un travail administratif qu'il semble judicieux de leur épargner. - Le garde-fou prévu par l'article 12 al. 1 AP-LPD, à savoir que le défunt n'a pas de son vivant interdit expressément la consultation et qu'aucun intérêt prépondérant du défunt ou d'un tiers ne l'empêche, constituent des protections insuffisantes en matière de secret médical. Il paraît

					en effet douteux que l'ensemble des patients soient informés, au début de chaque relation thérapeutique, de leur droit de s'opposer à la divulgation de leurs données après leur mort. Nous reconnaissons que la consultation de données médicales d'une personne décédée doit pouvoir être accordée dans des circonstances particulières, notamment en cas de suspicion d'erreur médicale ayant conduit à la mort du patient. Toutefois, même dans cette hypothèse, la transmission d'informations aux proches doit être strictement encadrée et se limiter aux seules informations nécessaires. En conséquence, l'article 12 AP-LPD ne peut pas subsister sous la forme proposée en ce qui concerne les données personnelles sur la santé.
IDS	LPD	14			De manière générale, les exceptions prévues par l'article 14 AP-LPD doivent être énoncées de manière plus restrictive. L'alinéa premier paraît ainsi trop flou et laisse la place à des abus. Par conséquent, nous proposons de tracer cette disposition. En raison des risques importants que pourraient causer un traitement défaillant de données personnelles sur la santé, il est en effet primordial qu'une personne soit informée lorsque de telles données la concernant sont traitées. Ainsi, certaines exceptions prévues par l'article 14 AP-LPD n'ont pas lieu d'être lorsqu'elles concernent des données personnelles relatives à la santé (voir ci-dessous les commentaires spécifiques sur les alinéas concernés).
IDS	LPD	14	2		L'IDS propose de reformuler cette disposition comme suit : ~~[1] Le responsable du traitement est délié du devoir d'information au sens de l'art. 13 lorsque la personne concernée dispose déjà des informations correspondantes.~~ [1] Le présent article ne s'applique pas aux données personnelles de santé et aux échantillons biologiques.
IDS	LPD	18			**L'IDS salue l'introduction d'un devoir de protection des données dès la conception et par défaut. Cette disposition doit absolument être maintenue.**

IDS	LPD	19		b	La situation appréhendée ici pourrait se révéler problématique en cas de changement du responsable du traitement ou du sous-traitant. Afin d'assurer le bon exercice du devoir d'informer les destinataires auxquels des données ont été communiquées, il serait judicieux d'obliger les responsables de traitement et les sous-traitants de communiquer la liste des personnes à qui des données ont été communiquées lors du changement de responsable du traitement ou de sous-traitant.
IDS	LPD	27	3	b	Même si elles sont accessibles à tout un chacun, les données personnelles d'une personne ne doivent pas être traitées par des organes fédéraux sans que ce traitement ne repose sur une base légale. Cette exception peut tout au plus être limitée au consentement de la personne concernée.
IDS	LPD	27	3	c	Cette exception n'est pas acceptable. Le traitement de données en vue de préserver des intérêts de tiers peut, à la rigueur, être admis dans des circonstances exceptionnelles. Toutefois, tel n'est pas le cas du traitement sans base légale et sans consentement de la personne concernée, dans l'unique intérêt de cette dernière. Cette disposition ouvrirait une brèche dangereuse pour justifier des traitements de données infondés, contre la volonté de la personne concernée.
IDS	LPD	30			Il serait bienvenu de préciser que la personne qui s'oppose à la communication de données personnelles par l'organe fédéral ne subira pas de conséquences négatives du simple fait de cette opposition.
IDS	LPD	31			L'occasion est saisie ici de rappeler que les dossiers médicaux qui seraient traités par les organes de la Confédération ne doivent pas pouvoir être conservés/archivés contre la volonté du patient, sauf en présence d'un motif justificatif suffisamment fondé. En particulier, un dossier médical ne doit pas être archivé contre la volonté d'un patient au seul motif qu'il constitue un document de la Confédération.
IDS	LPD	32			L'occasion de la révision de la LPD devrait être saisie pour traiter séparément les exigences posées en matière de traitement de données personnelles à des fins de planification et de statistique et le traitement de données personnelles à des fins de recherche. L'article 32 LPD devrait aussi viser les traitements de données par les organes fédéraux en matière de

					d'assurance qualité. Il devrait par conséquent être consacré aux traitements à des fins de planifications, d'assurance de qualité et de statistique, à l'exclusion des traitements à des fins de recherche qui doit faire l'objet d'un article séparé. Il convient par ailleurs d'opérer une distinction entre l'anonymisation et la publication sous une forme ne permettant pas d'identifier une personne (dans le sens de l'article 32 al. 1 let. d AP-LPD). Afin d'éviter tout risques de ré-identification, il serait plus judicieux de préférer la forme « anonymisée ». Par ailleurs, la communication de données sensibles à des personnes privées (art. 32 al. 1 let. b) doit être soumise à des conditions plus strictes. Nous sommes d'avis que les données ainsi communiquées doivent au moins être « codées » et que la clé de codage doit se trouver dans les seules mains l'organe fédéral concerné. L'article 32 LPD pourrait avoir la teneur suivante : « *Art. 32 Traitements à des fins de planification, d'assurance de qualité et de statistique* *[1] Les organes fédéraux sont en droit de traiter des données personnelles à des fins ne se rapportant pas à des personnes, notamment de planification, d'assurance qualité ou de statistique, si les conditions suivantes sont réunies :* *a. les données sont rendues anonymes dès que le but du traitement le permet et une ré-identification n'est matériellement pas possible;* *b. l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme codée ne permettant pas d'identifier les personnes concernées ;* *c. le destinataire ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises ;* *d. les résultats du traitement sont publiés sous une forme anonymisée.* *[2] Les art. 4, al. 3, 27, al. 1 et 2 et 29, al. 1 ne sont pas applicables.* » La recherche poursuit quant à elle des buts différents de la planification, de l'assurance qualité et de la statistique et présente de risques marqués pour les personnes dont les données sont traitées. Ce

					besoin de protection accru justifie la création d'un nouvel article qui traiterait spécifiquement des traitements de données personnelles par les organes fédéraux à des fins de recherche. Il serait judicieux de soumettre ce type de données aux exigences posées par loi fédérale relative à la recherche sur l'être humain (LRH). Par ailleurs, dans le contexte de la recherche, il est primordial de prendre en compte le consentement de la personne concernée. Il faut ainsi conditionner le traitement de données personnelles par des organes fédéraux à des fins de recherche à la condition que les personnes concernées ne soient pas opposées à une telle utilisation. Le nouvel article relatif à aux traitements à des fins de recherche (art. 32a) pourrait avoir la teneur suivante : « *Art. 32a Traitements à des fins de recherche* *[1] Les organes fédéraux sont en droit de traiter des données personnelles à des fins de recherche si les conditions suivantes sont réunies :* *a. les données sont rendues anonymes dès que le but du traitement le permet et une ré-identification n'est matériellement pas possible;* *b. les personnes concernées ne se sont pas opposées à une telle utilisation ;* *c. l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme codée ne permettant pas d'identifier les personnes concernées ;* *d. le destinataire ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises ;* *e. les résultats du traitement sont publiés sous une forme anonymisée.* *[2] Les art. 4, al. 3, 27, al. 1 et 2 et 29, al. 1 ne sont pas applicables.* *[3] Sont réservées les exigences de la loi fédérale relative à la recherche humaine du 31 septembre 2011.* »

IDS	LPD	51			Du point de vue du champ d'application territorial, il serait bienvenu de rappeler que les infractions pénales prévues par la LPD, en particulier celles qui ont pour objet la violation du devoir de diligence (art. 51 AP-LPD), s'étendent également aux actes commis à l'étranger, conformément à la théorie des effets adoptée par le Tribunal fédéral. Afin d'imposer en Suisse un droit de la protection des données suffisamment efficace et dissuasif, il serait judicieux d'inscrire dans la loi que les dispositions pénales de la LPD s'appliquent lorsque les données concernées ont été collectées en Suisse.
IDS	LPD	51a			L'avant-projet en consultation ne comprend pas de sanctions administratives propres à dissuader les entreprises actives dans le domaine. Nous proposons ainsi d'adopter une disposition analogue à celle de l'art. 83 du Règlement (UE) 2016/679 sur la protection des données et dont les sanctions devraient être analogues, à savoir : « *Section 8 Dispositions pénales* ***et administratives*** » « *Art. 51a Sanctions administratives* *Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives prononcées par le préposé pouvant s'élever jusqu'à 20 000 000 CHF ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu: …* »
IDS	LPD	52			L'intention de combler les lacunes de l'article 321 CP, en élargissant la violation du devoir de discrétion à tous les types de données (et non plus aux seules données sensibles), est à saluer. Cela dit, la notion de données personnelles « *secrètes* » reste peu précise. Il serait peut-être judicieux de la définir à l'article 3. Nous constatons par ailleurs qu'il existe toujours un problème de coordination entre les dispositions de la LPD et les dispositions pénales sur le secret professionnel (art. 321 CP) et le secret de fonction (art. 320 CP), notamment du point de vue des exceptions respectives à chacun de ces secrets.

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

nom/société	remarque / suggestion :
IDS	

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

nom/société	remarque / suggestion :
IDS	

Rapport explicatif : chap. 8 « Commentaire des dispositions »

nom/société	art.	remarque / suggestion :
IDS		

IG DHS
Interessengemeinschaft
Detailhandel Schweiz

Geschäftsstelle
Postfach
3001 Bern

Telefon 031 313 33 35
Fax 031 313 33 22
E-Mail info@igdhs.ch

www.igdhs.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
CH-3003 Bern

Basel, 4. April 2017

Vernehmlassung zum neuen Datenschutzrecht: Stellungnahme IG DHS

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit der Stellungnahme zu den angedachten Änderungen im Datenschutzrecht. Die Mitglieder der Interessengemeinschaft Detailhandel Schweiz (IG DHS) sind auf vielfältige Weise mit der Thematik des Datenschutzes konfrontiert und begegnen dieser schon seit Jahren auf kompetente und verantwortungsbewusste Weise.

Der Werkplatz Schweiz hat sich in den vergangenen Jahrzehnten auch dank eines hohen Digitalisierungsgrads unserer Wirtschaft erfolgreich positionieren können. Alle sind sich einig, dass wir heute erst am Anfang einer noch viel weitergehenden Entwicklung stehen: Es steht uns ein fundamentaler Wandel der künftigen (Welt-)Wirtschaft bevor. Dabei sind die Daten und die Datenbewirtschaftung der wertvollste Rohstoff. Wenn nun in der Schweiz mit einer restriktiven Regulierung des Datenhandlings neue Geschäftsmodelle verhindert werden, so gelangt der Werkplatz Schweiz schnell ins Hintertreffen. Die digitale Wirtschaft findet global statt und spielt sich dort ab, wo auch ein optimaler Regulierungsrahmen besteht. So zeigen z.B. Google, Apple, Cisco, Alibaba auf, wohin es in Zukunft geht: Die Wirtschaft wird immer enger verknüpft mit einem tiefgreifenden Einsatz der Informations- und Kommunikationstechnik. Von dieser Entwicklung profitieren diejenigen Wirtschaftsstandorte, welche massvolle, aber zurückhaltende Regulierungen i.S. Datenschutz haben.

Das neue DSG ist daher ganz grundsätzlich zu überarbeiten und zu entschlacken. Alleine die europäischen verbindlichen Vorschriften i.S. Datenschutz gehen eigentlich schon zu weit, wenn man den weltweiten Markt der digitalen Wirtschaft betrachtet. Dass darüber hinaus noch zusätzliche schweizerische Regulierungen vorgeschlagen werden, geht eindeutig zu weit. Die IG DHS lehnt daher dezidiert sämtliche Regulierungen ab, welche über die EU-Regulierungen hinausgehen. Diese vorgeschlagene Swiss Finish-Gesetzgebung gefährdet die Wettbewerbsfähigkeit des digitalen Wirtschaftsstandorts Schweiz.

Zu den Vernehmlassungsvorlagen äussert sich die IG DHS im Grundsatz wie folgt:

JA zur Übernahme der Richtlinie (EU) 2016/680 im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen
Die Übernahme ist im Rahmen des Schengen-Abkommens verpflichtend und steht deshalb für die IG DHS ausser Frage.

JA zur Ratifizierung des revidierten Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108)
Die Ratifizierung ist massgebend für den Angemessenheitsentscheid der EU-Kommission zum Datenschutzniveau in der Schweiz. Aus der Sicht der IG DHS ist sie ebenfalls unbestritten.

Totalrevision des Datenschutzgesetzes (DSG)
Die EU-Kompatibilität des neuen DSG ist im Rahmen der Totalrevision zu gewährleisten. Darüber hinausgehende Regelungen (Swiss Finish) sind strikte zu vermeiden. Die künftig möglichen Datenbewirtschaftungsformen sind eine Chance für den schweizerischen Werkplatz. Das angedachte DSG verunmöglicht jedoch einen liberalen und gleichzeitig sicheren Umgang mit Daten. Dies gefährdet die Wettbewerbsfähigkeit der Schweiz im Bereich digitale Wirtschaft.

Zur Totalrevision des DSG finden Sie im Folgenden die allgemeinen Forderungen der IG DHS sowie im beiliegenden Formular die konkreten Anträge für den Gesetzestext.

1. **Änderungen auf das beschränken, was im internationalen Kontext zwingend nötig ist**

- Das EU-Recht muss für das neue Schweizer DSG massgebend sein. Viele Schweizer Unternehmen sind heute in irgendeiner Weise international tätig oder bearbeiten zumindest Daten in einem internationalen Kontext. Somit ist die europäische Datenschutzgrundverordnung (DSGVO) für viele Unternehmen ohnehin operativ relevant. Die Schweizer Gesetzgebung muss deshalb grundsätzlich gleichwertig ausgestaltet werden.
- Dabei gilt es auch den von der DSGVO gegebenen Handlungsspielraum auszunutzen und dort liberalere Regeln vorzusehen, wo dies im Schweizer Kontext sinnvoll und der Sache dienlich ist. Dies ist insbesondere bei den aufsichtsrechtlichen Bestimmungen (Kompetenzen des Beauftragten) der Fall.

2. **Interpretationsspielraum in der Folgeregulierung klären**

- Die hohe Ambivalenz des Gesetzestextes verunsichert. Zum jetzigen Zeitpunkt ist es insgesamt sehr schwierig, die betrieblichen Auswirkungen der Vernehmlassungsvorlage detailliert abzuschätzen, da das vorliegende Gesetzt lediglich ein Rahmengesetz sein soll.
- Die risikobasierte, prinzipienorientierte Ausgestaltung des neuen DSG wird seitens IG DHS begrüsst. Es gilt jedoch im Botschaftstext, im parlamentarischen Prozess, bei der Ausarbeitung der Verordnungen und in zukünftigen Empfehlungen der guten Praxis auf eine klare Linie zu achten. Der vorliegende Gesetzesentwurf grenzt insbesondere noch zu unklar das Pflichtenheft von "Verantwortlichem" und "Auftragsbearbeiter" ab.
- Die Rechtssicherheit für die betroffenen Unternehmen muss letztlich gewährleistet sein. Die Folgeregulierungen dürfen für die betroffenen Unternehmen nicht plötzlich unverhältnismässige Investitions- und Betriebskosten nach sich ziehen. Gegebenenfalls sind zu einzelnen Massnahmen auch vertiefende Regulierungsfolgeabschätzungen erforderlich.

3. **Bedarfsgerechte, konsumentenfreundliche Auskunfts- und Informationspflichten**

- Die IG DHS befürwortet es, dass die Transparenz und Rückverfolgbarkeit einzelner Bearbeitungsvorgänge für die Konsumentinnen und Konsumenten verbessert wird. Aus Sicht der IG DHS wird dieses Ziel jedoch verfehlt, wenn ihnen öfters und immer mehr Informationen zu einzelnen Datenbearbeitungsvorgängen zur Verfügung gestellt werden. Es ist sogar davon auszugehen, dass dies zu einer Überforderung und Desensibilisierung der betroffenen Personen führt. Mit dem neuen DSG würden die Menge und die Komplexität der zu prüfenden Informationen nochmals massiv zunehmen. Im Verhältnis zum erwarteten Nutzen stellt dies einen unverhältnismässigen administrativen Mehraufwand dar.

- Stattdessen hat das neue DSG auf eine verbesserte *allgemeine und prinzipielle* Information abzuzielen, so dass sich eine betroffene Person *vorab* der Konsequenzen einer Datenpreisgabe bewusst wird. Die vorgesehenen Informations- und Auskunftspflichten sind entsprechend sinnvoll einzugrenzen. Der Katalog der mitzuteilenden Informationen muss sich dabei zwingend eins zu eins an den Anforderungen in der EU zu orientieren.

4. Wirtschaftsfreundliche und pragmatische Mitwirkungspflichten

- Die IG DHS fordert, dass der Umfang einer Datenschutzfolgeabschätzung auf ein sinnvolles, sachgerechtes Mass beschränkt wird (z.B. als vorgelagertes Datenbearbeitungsreglement). Was für die Pflichten der Unternehmen gegenüber den Konsumentinnen und Konsumenten gilt, muss deshalb auch für die Meldepflichten an den Beauftragten gelten: Weniger ist mehr. Ausserdem gilt es kurze, wirtschaftsfreundlich Ordnungsfristen für die Bearbeitung durch den Beauftragten im Rahmen der Folgeregulierung festzusetzen.
- Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse an den Beauftragten ist sodann stark einzuschränken. Sie erfasst weit mehr Fälle als die DSGVO. Die Pflicht ist daher auf Verstösse mit gravierenden Folgen zu beschränken. Im Sinne einer modernen Compliance-Gesetzgebung muss die Meldung beim Beauftragten den Schutz vor Sanktionen zur Folge haben.
- Der Beauftragte seinerseits soll seine neuen Aufgaben und Kompetenzen unter den gleichen personellen und finanziellen Voraussetzungen wie bis anhin erfüllen. Zusätzliche Mittel führen aus der Sicht der IG DHS tendenziell dazu, dass die Behörde zur eigenen Legitimation in Aktionismus verfällt.

5. Freiwillige branchenspezifische Regeln vorsehen

- Die kommerzielle Auswirkung der Datenbearbeitung, der Aufwand der Information und des Einholens einer Einwilligung sind je nach Branche sehr unterschiedlich. Die IG DHS begrüsst es daher, dass mittels Empfehlungen der guten Praxis eine verstärkte Selbstregulierung stattfinden soll. So gilt es sicher zu stellen, dass das neue DSG nicht zu einer "one size fits all"-Lösung wird.
- Im Detailhandel sind z.B. übliche Kundenbindungsprogramme derzeit noch vorwiegend "offline". Eine Änderung der Datenschutzbestimmungen (in den AGB) und das folglich notwendige Einholen des Einverständnisses der betroffenen Personen sind mit einem sehr grossen Aufwand verbunden (u.a. Medienmitteilung, Postversand, E-Mail-Versand). Demgegenüber kann etwa ein Social-Media-Anbieter Änderungen an den AGB und das Einholen des Einverständnisses sehr viel schneller, einfacher und kostengünstiger durchführen.
- Soll der Ansatz der Selbstregulierung konsequent umgesetzt werden, müssen die Empfehlungen der guten Praxis als freiwillige Branchenvereinbarungen ausgestaltet werden. Die Ausarbeitung der Branchenstandards muss von den betroffenen Unternehmen und Branchen selbst erarbeitet werden. Dem Beauftragten soll dabei ein Mitwirkungsrecht eingeräumt werden. Dieser praxisgerechte, effiziente Lösungsansatz hat sich verschiedenerorts bereits sehr bewährt (Swiss Pledge (Werbeverhalten gegenüber Kindern); Plastiksackverbot usw.).

6. Geschäftsgeheimnisse schützen

- Die Vernehmlassungsvorlage schützt Geschäftsgeheimnisse nicht ausreichend. Zwar sind Bestimmungen vorgesehen, die das Aufschieben, Einschränken oder den Verzicht der Information oder Auskunft zulassen, wenn "eigene überwiegende Interessen" vorliegen. Der erläuternde Bericht zur Vorlage lässt jedoch vermuten, dass dem Bund hier eine Handhabung vorschwebt, die in der Praxis schlicht nicht umsetzbar wäre, ohne dass sensitive Informationen bekannt gegeben werden müssten. Auch wäre wiederum der Informations-Mehrwert für die betroffenen Personen aus der Sicht der IG DHS sehr gering.

- Die IG DHS fordert deshalb, dass geschäftlich sensitive Bearbeitungsvorgänge von vornherein von einer etwaigen Information oder Auskunft ausgenommen werden können.

7. Alleinige Aufsicht des Beauftragten in der Schweiz sicherstellen

- Die DSGVO tritt im Mai 2018 in Kraft, das revidierte DSG wird zu gegebenem Zeitpunkt folgen. Die Parallelität der beiden gesetzlichen Rahmen wirft die Frage der aufsichtsrechtlichen Zuständigkeit auf: Es muss gewährleistet werden, dass der Beauftragte in der Schweiz die alleinige aufsichtsrechtliche Hoheit hat, egal ob in einem bestimmten Fall das Schweizer DSG oder die DSGVO Anwendung zur Anwendung kommt.
- Die IG DHS begrüsst es, dass sich Bundesrat und Parlament im Rahmen der Motion 16.3752 mit dieser Problematik befassen und auch ihre Bereitschaft signalisiert haben, in dieser Sache Sondierungsgespräche mit der EU zu führen.

8. Umfassende Überarbeitung der strafrechtlichen Bestimmungen nötig

Die IG DHS fordert aufgrund der folgenden Erwägungen eine umfassende Überarbeitung der vorgesehenen Strafbestimmungen:

- **Grundsätzliches:** Die Strafbestimmungen verstossen gegen strafrechtliche Grundprinzipien. Die vorgesehenen Mitwirkungspflichten (insbesondere die Meldepflicht bei Datenschutzverstössen) kämen faktisch einer Selbstanzeige gleich, was mit Blick auf das Selbstbelastungsverbot besonders stossend ist.
- **Persönliche Strafbarkeit von Mitarbeitenden:** Die IG DHS lehnt die vorgesehenen individualstrafrechtlichen Sanktionen ab. Sie führen zu einer Kriminalisierung der mit dem Datenschutz betrauten Mitarbeiter. Die gesetzlich gegebenen Spielräume bei der Datenbearbeitung werden dann aus Angst vor persönlicher Bestrafung nicht ausgenutzt und es wird ein Denunziantentum innerhalb der Unternehmen gefördert. Ausserdem geraten Mitarbeitende in einen nicht hinnehmbaren Zielkonflikt, wenn sie zwischen der Wahrung von Geschäftsgeheimnissen und der Einhaltung ihrer Pflichten aus dem Datenschutzrecht abwägen müssen.
- **Verwaltungssanktionen gegen Unternehmen:** Im Gegenzug sind die Möglichkeiten zu Verwaltungssanktionen gegen Unternehmen auf verhältnismässige Art und Weise zu erweitern. Dieser Ansatz ist auch in der EU üblich, steht im Einklang mit anderen Gesetzen (KG, UWG, FMG und BEHG) und ist sachgerecht. Dabei ist darauf zu achten, dass die Sanktion zwar wirksam und abschreckend, aber auch angemessen ist. Als angemessen erachten wir dabei eine Busse von höchstens CHF 500‘000.- resp. höchstens 250'000.- bei leichtem Verschulden.

Wir danken Ihnen für die Berücksichtigung unserer Argumente und stehen Ihnen für Rückfragen jederzeit zur Verfügung.

Freundliche Grüsse

Beat Flury
Leiter IG DHS AG Binnenmarkt

Salome Hofer
Mitglied IG DHS AG Binnenmarkt

Beilage: Fragebogen IG DHS zur Totalrevision DSG

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Interessengemeinschaft Detailhandel Schweiz

Abkürzung der Firma / Organisation : IG DHS

Adresse : Geschäftsstelle, Postfach 5815, 3001 Bern

Kontaktperson : Patrick Marty, Geschäftsführer

Telefon : +41 31 313 33 33

E-Mail : info@igdhs.ch

Datum : 04. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
IG DHS	**<u>Vorbemerkung zu den Anträgen im Gesetzestext:</u>** Wir verweisen an dieser Stelle auf unser Begleitschreiben zur vorliegenden Stellungnahme.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
IG DHS	VE-DSG	2	2		**Antrag:** Die Nichtanwendbarkeit des DSG auf hängige Verfahren gemäss Art. 2 Abs. 1 lit. c DSG fehlt und ist ins neue Recht zu übernehmen. **Begründung:** Es kann nicht angehen, dass die gegnerische Partei während hängiger Verfahren Auskunftsbegehren stellen kann. Dies hätte zur Folge, dass die so zur Auskunft verpflichtete Partei sich selbst belasten müsste (Verstoss gegen den nemo tenetur-Grundsatz).
IG DHS	VE-DSG	3		f	**Antrag:** *Profiling: jede automatisierte Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;* **Begründung:** Die Definition von Profiling geht über das EU-Recht hinaus und soll jener der DSGVO angeglichen werden. Die Formulierung "um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen" muss in der Folge-Regulierung eng eingegrenzt und sinnvoll konkretisiert werden.
IG DHS	VE-DSG	4	3		**Antrag:** *Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.* **Begründung:**

					Der Begriff "klar" ist zu streichen, da er ambivalent ist Die Interpretationshoheit des Verwendungszwecks muss beim Verantwortlichen liegen und darf nicht von vornherein durch das Gesetz zu eng abgesteckt sein
IG DHS	VE-DSG	4	5		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Es ist nicht im Interesse eines Unternehmens, veraltete oder falsche Daten zu bearbeiten, da dies das Ergebnis der Bearbeitung verfälschen oder gar unbrauchbar machen kann. Es besteht bereits ein konkreter betriebswirtschaftlicher Anreiz, möglichst wahrheitsgetreue Daten zu verwenden, so dass eine gesetzliche Bestimmung hierzu redundant wäre.
IG DHS	VE-DSG	4	6		**Antrag 1:***Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen.* **Begründung 1:** Das Erfordernis der Einwilligung geht über die EU-Regelung hinaus und ist deshalb zu streichen. **Antrag 2:** Die Einholung der Einwilligung muss einmalig und in allgemeiner Weise möglich sein (z.B. durch Ankreuzen eines Feldes, gem. Hinweis im Erläuternden Bericht), mindestens solange die gleiche Datengrundlage für die Bearbeitung verwendet wird. Dies ist auf Verordnungsebene zu gewährleisten. **Begründung 2:** Das häufigere Einholen einer Einwilligung (besonders einer ausdrücklichen) ist für die betroffenen Unternehmen sehr aufwändig und verbessert die Transparenz für die Konsumentinnen und Konsumenten nicht. Zudem ist die Massnahme besonderes kostenintensiv für Angebote, die nicht rein Web-basiert sind (z.B. Ist das Einholen der Einwilligung zu einer AGB-Änderung bei einer Kundenkarte massiv teurer als bei einer

					Suchmaschine oder einem Social-Media-Account). Dies ist diskriminierend für einzelne Wirtschaftszweige.
IG DHS	VE-DSG	5	5		**Antrag:** *Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens dreissig Tage ~~sechs Monate~~ nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.* **Begründung:** Die Frist von sechs Monaten, die zudem durch die Nachforderung von Informationen durch den Beauftragten beliebig verlängerbar ist, macht ein Genehmigungsverfahren nicht sinnvoll umsetzbar und führt zu unzumutbaren Verzögerungen bei Auslandtransfers. Eine Frist von dreissig Tagen (wie bisher) genügt.
IG DHS	VE-DSG	5	6		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Die Pflicht zur Information des Beauftragten geht über die Anforderungen der EU-Gesetzgebung (DSGVO) hinaus und wird deshalb abgelehnt. Sie bedeutet eine nicht akzeptable Mehrbelastung für alle Unternehmen und generiert zudem eine für den Beauftragten (zeitlich und inhaltlich) nicht sinnvoll zu bewältigende Informationsflut – ohne dass dabei ein Mehrwert für den Datenschutz geschaffen wird.
IG DHS	VE-DSG	6	1	a	**Antrag:** *In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:* *a. die betroffene Person ~~im Einzelfall~~ eingewilligt hat;* **Begründung:** Die Einzelfallbetrachtung führt in der Praxis zu Unklarheiten da meistens die Einwilligung für einen Zweck

					eingeholt wird und nicht für eine einzelne Übermittlung von Personendaten. Wenn also ein Unternehmen Daten ins Ausland bekannt gibt, soll es hierfür im Voraus und in allgemeiner Weise die Einwilligung einholen können (vgl. Antrag zu Art. 4, Abs. 6)
IG DHS	VE-DSG	6	2		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Die Meldepflicht von Datentransfers geht zu weit und ist nicht sinnvoll. Es kann nicht sein, dass der Beauftragte über solche Geschäftsgeheimnisse, welche wohl nicht einmal datenschutzrelevant sind, informiert werden muss. Es wird zudem kaum über die Kapazitäten verfügen um die Meldungen zielführend zu verarbeiten. Zudem ist eine solche Bestimmung im EU-Recht (DSGVO) nicht vorgesehen. Entgegen den Ausführungen im Erläuternden Bericht (S. 51/52) wird dies auch vom Entwurf zur Revision des Übereinkommens SEV 108 nicht zwingend verlangt.
IG DHS	VE-DSG	7	2		**Bemerkung:** Bei der Präzisierung durch den Bundesrat muss die Rechtssicherheit für den Verantwortlichen bewahrt werden. Insbesondere ist darauf zu achten, dass der Auftragsbearbeiter sich nicht hinter seinem Auftraggeber verstecken kann. **Antrag:** *Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit ~~und die Rechte der betroffenen Person~~ zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.* **Begründung:** Es ist unklar, um welche Rechte es hier geht und welche Pflichten dem Auftragsbearbeiter übertragen werden sollen. Es ist völlig unrealistisch und unverhältnismässig, wenn der Auftragsbearbeiter sämtliche Rechte der betroffenen Person gewährleisten muss.

IG DHS	VE-DSG	8	1-2		**Bemerkung:** Die IG DHS begrüsst es, dass gemäss VE-DSG mittels Empfehlungen der guten Praxis eine verstärkte Selbstregulierung stattfinden soll. Die konkret vorgeschlagene Bestimmung läuft diesem Zweck jedoch gerade zuwider. Es kann nicht angehen, dass dem Beauftragten ein Genehmigungsvorbehalt zukommt – sonst handelt es sich letztlich um eine einseitige Auslegung des DSG durch den Beauftragten. Damit die Konkretisierung der datenschutzrechtlichen Pflichten sich als praxistauglich erweist, müssen Formulierungsvorschläge von den betroffenen Unternehmen und Branchen selbst erarbeitet werden. Soll der Ansatz der Selbstregulierung konsequent umgesetzt werden, muss die Initiative für Empfehlungen der guten Praxis daher von den interessierten Kreisen (Unternehmen und Branchen) selbst ausgehen. In anderen Rechtsgebieten haben sich Branchenvereinbarungen auf freiwilliger Basis als zielführend erwiesen (vgl. etwa die Branchenvereinbarung Plastiksäcke). Die Bestimmung ist dahingehend anzupassen, dass Unternehmen und Branchen das Recht haben, selbständig Branchenvereinbarungen auszuarbeiten. Statt einem Genehmigungsvorbehalt kommt dem Beauftragten ein Mitwirkungsrecht zu.
IG DHS	VE-DSG	9			**Antrag:** Die Empfehlungen sollen lediglich die Vermutung begründen, dass das Gesetz eingehalten wird (keine Fiktion). **Begründung:** Eine Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung der Datenschutzvorschriften schliesst, ist nicht zielführend und wäre rechtsstaatlich problematisch. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig oder unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.
IG DHS	VE-DSG	13			**Bemerkung:** Aus der vorgeschlagenen Formulierung von Art. 13 VE-DSG geht zu wenig eindeutig hervor, welche Beschaffungsvorgänge von der Informationspflicht betroffen sind. In der Botschaft ist klar festzuhalten, dass nicht jede einzelne Datenbeschaffung eine Informationspflicht auslösen kann. Insbesondere dürfen die in Art. 13 Abs. 2 lit. b VE-DSG genannten Kategorien von Personendaten nicht zu eng gefasst werden.

IG DHS	VE-DSG	13	1		**Antrag:** *Der Verantwortliche informiert die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.* **Begründung:** Die Gesetzesformulierung gemäss Vernehmlassungsvorlage hätte zur Folge, dass KundInnen regelrecht mit Informationen überflutet würden. Eine Informationspflicht ist daher nur bei der Beschaffung von besonders schützenswerten Personendaten angezeigt.
IG DHS	VE-DSG	13	3		**Antrag:** *Werden Personendaten Dritten für deren eigene Verwendung bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.* **Begründung:** Die Weitergabe von Personendaten an Dritte im Rahmen von Art. 7 VE-DSG soll, wie im geltenden Recht (Art. 10*a* DSG), nicht der Informationspflicht unterliegen. Andernfalls müsste der Verantwortliche über den Beizug sämtlicher Hilfspersonen informieren.
IG DHS	VE-DSG	13	4		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Die Bekanntgabe der Identität des Auftragsbearbeiters stellt gegenüber dem EU-Recht eine Besonderheit dar und wird deshalb von der IG DHS abgelehnt (Swiss Finish).
IG DHS	VE-DSG	14	4	a	**Antrag:** *Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten:*

					a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht konzernfremden Dritten bekannt gibt; **Begründung:** Die Berufung auf ein überwiegendes privates Interesse muss bei der Datenweitergabe unter Konzerngesellschaften möglich sein, ansonsten mit einem enormen administrativen Mehraufwand zu rechnen wäre, der nicht zur Transparenz beiträgt.
IG DHS	VE-DSG	15	1		**Antrag:** *Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese ~~rechtliche Wirkungen oder~~ erhebliche Auswirkungen auf die betroffene Person hat.* **Begründung:** Die Voraussetzung für eine Information soll sich auf erhebliche Auswirkungen beschränken, so wie dies in der EU auch der Fall ist. Die Bedeutung von automatisierten Einzelentscheidungen wird in Zukunft weiter zunehmen. Es darf diesbezüglich keine gesetzlichen Vorschriften geben, welche die Kosten aller automatisierten Vorgänge schon im Voraus stark erhöhen. Unternehmen, die automatische Bearbeitungsvorgänge implementieren, müssen die Sicherheit haben, dass die entsprechende persönliche Auskunftspflicht nicht in jedem Bagatell-Fall erfüllt werden muss, sondern nur wenn dies tatsächlich dem Datenschutz dient. In diesem Sinne ist der Begriff "rechtliche Auswirkungen" zu streichen.
IG DHS	VE-DSG	15	2		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Es ist zu befürchten, dass ein Recht zur "Äusserung" faktisch zu einer Begründungspflicht führt und damit Vertragsfreiheit einschränkt. Das ist ein Anliegen des Konsumentenschutzes, das nicht ins Datenschutzrecht gehört.

IG DHS	VE-DSG	16	1		**Antrag:** *Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen ~~erhöhten~~ Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen.* **Begründung:** Wie auch im EU-Recht, soll die Folgeabschätzung nur bei einem hohen Risiko notwendig werden. Auch ist der Verweis auf die Grundrechte zu entfernen – Es ist (wie gemäss geltendem Recht) nicht die Aufgabe eines privaten Verantwortlichen, die Grundrechte betroffener Personen zu schützen, sofern diese Grundrechte nicht in einzelnen Anforderungen des DSG Ausdruck gefunden haben. Die IGHDS investiert bereits heute viel in den Datenschutz – dies wurde seitens des Beauftragten mehrfach gewürdigt. Trotz diesen guten Voraussetzungen hätte die vorgesehene Vorschrift der Datenschutz-Folgeabschätzung erhebliche Kosten-Auswirkungen, sofern die genannte Einschränkung nicht erfolgt. Die Datenschutzfolgeabschätzung darf (dem EU-Recht entsprechend!) nicht mehr als ein zeitlich vorgelagertes Datenbearbeitungsreglement sein.
IG DHS	VE-DSG	16	3-4		**Antrag:** Beide Bestimmungen ersatzlos streichen. **Begründung:** Beide Bestimmungen gehen über die Regelungen des EU-Rechts hinaus und führen zu einem hohen Mehraufwand mit geringem Zusatznutzen für die Konsumentinnen und Konsumenten. Die Frist von drei Monaten zur Erhebung von Einwänden kann zudem eine unnötige Verzögerung bei Einführung neuer Geschäftsmodelle bewirken.
IG DHS	VE-DSG	17			**Antrag 2:** Der Begriff der Unverzüglichkeit in Abs. 1 ist genau zu klären. Ebenso sind die Pflichten des Auftragsbearbeiteter jene des Verantwortlichen abzustimmen.

					Begründung: Auch hier fordert die IG DHS eine massvolle Regulierung, so dass nicht jede Kleinigkeit eine Meldung nach sich zieht. Dies wäre aus Sicht der betroffenen Personen, der Unternehmen und letztlich auch des Beauftragten nicht zweckmässig aufgrund der resultierenden Informationsflut. Denkbar wäre ein analoger Prozess wie bei einem Produkt-Rückruf durch das BLV oder das BAG – in diesem Bereich hat sich ein risikobasierter Ansatz (da abgestuft für verschiedene Situationen!) und ein funktionierender Austausch zwischen Bundesorganen und Wirtschaft etabliert.
IG DHS	VE-DSG	18	1		**Antrag 1:** Der Begriff "angemessene Massnahmen" ist in der Verordnung auf prinzipielle Weise zu konkretisieren, so dass die betroffenen Unternehmen einerseits Rechtssicherheit haben und andererseits keine unverhältnismässigen Massnahmen umzusetzen sind. **Begründung 1:** Die IG DHS befürwortet einen besseren Datenschutz "ex ante", jedoch nicht ohne eindeutige Definition der "Angemessenheit". Die Marktbearbeitung muss weiterhin unter stabilen Rahmenbedingungen stattfinden können. **Antrag 2:** *Der Verantwortliche ~~und der Auftragsbearbeiter sind~~ ist verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen.* **Begründung 2:** Der Einbezug der Auftragsbearbeiter in die vorliegende Bestimmung geht über die Regelung im EU-Recht hinaus. Sie wird deshalb von der IG DHS abgelehnt.
IG DHS	VE-DSG	18	2		**Bemerkung:** "Privacy by Default" muss so praxisnah wie möglich umgesetzt werden. Dies beinhaltet auch die Sicherstellung der Planungs- und Rechtssicherheit für Unternehmen, die beispielsweise in Kundenbindungspro-

					gramme investieren.
IG DHS	VE-DSG	19		a, b	**Antrag:** *Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet:* *(…)* ~~*b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede eine wesentliche Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.*~~ **Begründung:** Inhalt und Ausmass der Pflicht zur Dokumentation der Datenbearbeitung gemäss lit. a soll auf das Führen eines Verzeichnisses aller Datenbearbeitungen, für die der Verantwortliche direkt zuständig ist, beschränkt werden. Es wäre absolut unverhältnismässig, eine umfassende und detaillierte Dokumentation der Datenbearbeitung zu verlangen, insbesondere auch vor dem Hintergrund, dass ein Verstoss gegen die Dokumentationspflicht nach dem VE-DSG sanktioniert werden kann. Ausserdem sieht das EU-Recht keine derart weitgehende Informationspflicht vor.
IG DHS	VE-DSG	20	1		**Bemerkung** Es fehlt eine Bestimmung zur Bekämpfung des Missbrauchs des Auskunftsrechts, insbesondere für die zweckentfremdete Nutzung zur Beweismittelausforschung. Dies ist umso stossender, da Auskunftsbegehren de lege nie unverhältnismässig sein können, sprich auch untergeordnete Datenschutzinteressen für einen Auskunftsanspruch ausreichen. Es sind daher weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. durch die Ergänzung von Art. 21 VE-DSG um einen weiteren Ausnahmetatbestand). **Antrag:** *Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.*

					Begründung: Die Möglichkeit einer Kostenbeteiligungspauschale soll gemäss geltendem Recht weitergeführt werden (Art. 2 VDSG).
IG DHS	VE-DSG	20	2	b, c, d, e, f	**Antrag:** *Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: (…)* *f. die verfügbaren Angaben über die Herkunft der Personendaten, sofern diese nicht direkt bei der betroffenen Person beschafft wurden; (…)* **Begründung:** Wenn die Personendaten bei der betroffenen Person selbst beschafft wurden, ist ein zusätzliches Auskunftsrecht über die Datenherkunft redundant.
IG DHS	VE-DSG	20	3		**Antrag:** Die Bestimmung ist ersatzlos zu streichen. **Begründung:** Die Pflicht zur Begründung jeglicher Entscheide (nicht nur automatisierte Einzelentscheide) greift massiv in die Freiheit eines Unternehmens ein und geht über die Erfordernisse der DSGVO hinaus.
IG DHS	VE-DSG	21			**Antrag:** Die Berufung auf überwiegende private Interessen muss zulässig sein. Dies gilt insbesondere für die Datenweitergabe innerhalb des Konzerns. **Begründung:** Siehe Begründung Antrag IG DHS zu Art. 14 Abs. 4 lit. a VE-DSG.

IG DHS	VE-DSG	23	2	d	**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Das Erfordernis der Einwilligung geht über die EU-Regelung hinaus und ist deshalb zu streichen.
IG DHS	VE-DSG	23	3		**Bemerkung:** Das Opt-out-Recht darf nicht zu einer Verunmöglichung oder Einschränkung des mitgeteilten Zweckes führen. Beispielsweise kann eine Kundenkarte nicht sinnvoll genutzt werden, wenn die betroffene Person die Zustimmung für die in den Geschäftsbedingungen vorgesehene Datenbearbeitung entzieht. Wer den in den AGB vorab beschriebenen Datenerhebungen und –bearbeitungen zustimmt, soll daher nachträglich diese Zustimmung nicht teilweise entziehen können. Es soll nur ein vollständiger Rücktritt möglich sein, da sonst das entsprechende Angebot nicht mehr sinnvoll genutzt werden kann.
IG DHS	VE-DSG	24	2	a	**Bemerkung:** Der Rechtfertigungsgrund des Abschlusses und der Abwicklung des Vertrags sollte auch die Bearbeitung von Daten weiterer, in den Vertrag involvierter Personen umfassen (z.B. Kontaktpersonen für Rückfragen).
IG DHS	VE-DSG	41	5		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:** Es verletzt die Geheim- und Privatsphäre des Unternehmens, wenn die Anzeige erstattende Privatperson über das Ergebnis einer allfälligen Untersuchung informiert wird.
IG DHS	VE-DSG	44	3		**Antrag:** Bestimmung ersatzlos streichen. **Begründung:**

					Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben. Die Erfahrungen haben gezeigt, dass der Beauftragte vorsorgliche Massnahmen auch ohne vertieftes Abwägen der Folgen beantragt. Eine unabhängige Überprüfungsmöglichkeit ist daher entscheidend. Bis diese stattfindet, muss eine aufschiebende Wirkung bestehen.
IG DHS	VE-DSG	50-55			**Antrag:** Es sind primär verwaltungsrechtliche Sanktionen für Unternehmen vorzusehen. Lediglich subsidiär soll eine strafrechtliche Verfolgung der Mitarbeitenden bei Vorsatz möglich sein. Die maximale Bussenhöhe für Unternehmen ist auf CHF 500'000.- resp. bei leichtem Verschulden auf CHF 250'000.- zu begrenzen. Der Strafenkatalog ist mit jenem der DSGVO abzugleichen. **Begründung:** Die vorgesehene persönliche Strafbarkeit ist weder verhältnismässig noch zielführend und führt in Unternehmen zu einer Denunziationskultur. Dem Ziel – einem hohen Datenschutzniveau – ist in einem verwaltungsrechtlichen Sanktionssystem besser gedient. Ferner müssen die in Art. 50-55 zitierten Pflichten genauer umschrieben werden, um dem strafrechtlichen Bestimmtheitsgebot gerecht zu werden. Durch die primäre Strafbarkeit der Unternehmen mit maximalen Bussen von CHF 500'000.- resp. CHF 250'000.- kannsichergestellt werden, dass Sanktionen wirksam und abschreckend, aber auch angemessen sind.
IG DHS	VE-DSG	52			**Antrag:** Die Bestimmungen zur Schweigepflicht sollen gemäss geltendem DSG belassen werden. **Begründung:** Für die Verschärfung der heute in Art. 35 DSG beschriebenen Schweigepflicht besteht kein Anlass. Es ist nicht nachvollziehbar, wieso z.B. der Onlinehandel den gleich weitreichenden Geheimhaltungspflichten wie etwa ein Arzt unterliegen soll. Ausserdem stellt Art. 52 VE-DSG mit der Bezugnahme auf "geheime Personendaten" auf einen Begriff ab, ohne diesen näher zu definieren.
IG DHS	VE-DSG	59			**Antrag:**

					Die Übergangsfrist von zwei Jahren ist generell zu gewähren. **Begründung:** Eine generelle Übergangsfrist von zwei Jahren ist angemessen und EU-konform (DSGVO).

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung

Amstutz Jonas BJ

Von: walter.stuedeli <walter.stuedeli@ig-ehealth.ch>
Gesendet: Dienstag, 4. April 2017 20:48
An: Amstutz Jonas BJ
Cc: Urs Stromer; mrufenac@cisco.com
Betreff: 20170404_Eingabe_Datenschutzgesetz_IG-eHealth.docx
Anlagen: 20170404_Eingabe_Datenschutzgesetz_IG-eHealth.docx

Sehr geehrter Herr Amstutz

Gerne sende ich Ihnen fristgemäss die Eingabe der IG eHealth zum Datenschutzgesetz. Darf ich Sie bitten, mir den Erhalt zu bestätigen?

Mit bestem Dank und freundlichen Grüssen

Walter Stüdeli

_____

Interessengemeinschaft eHealth
c/o Köhler, Stüdeli & Partner GmbH
Amthausgasse 18
3011 Bern

Walter Stüdeli, Geschäftsführer
lic.rer.pol./EMScom
Geschäft +41 31 560 00 24
Mobile +41 79 330 23 46

www.ig-ehealth.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Interessengemeinschaft eHealth

Abkürzung der Firma / Organisation : IG eHealth

Adresse : Amthausgasse 18, 3011 Bern

Kontaktperson : Walter Stüdeli, Geschäftsführer

Telefon : 031 560 00 24

E-Mail : walter.stuedeli@ig-ehealth.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
IG eHealth	Die Revsion des DSG hat zum Zweck, sich an die EU-Verordnung EU 2016/679 anzunähern, was im Grundsatz sinnvoll ist. Die Vorgaben sollten möglichst schlank gehalten werden, damit kein unnötiger Mehraufwand entsteht.
IG eHealth	Das DSG ist für das Gesundheitswesen sehr wichtig, der Gesetzesentwurf sollte auf die spezifischen Gegebenheiten adaptiert werden.
IG eHealth	Zu definieren ist, wie Spezialgesetzen wie dem Humanforschungsgesetz und dem ePatientendossier-Gesetz bezüglich des Datenschutzes umgegangen werden soll. Die IG eHealth schlägt vor, dass die lex specialis den Vorrang erhalten und im DSG explizit genannt werden.
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
IG eHealth	DSG	3		f	Im Gesetz sollte unter den Begriffen klarer umschrieben werden, welche Elemente zum «Profiling» gehören (Analyse von Lebensdaten, medizinische Befunde)
IG eHealth	DSG	4	3 und 4		Die Datenaufbereitung und Datenarchivierung ist in den kantonalen Gesetzen geregelt (in der Regel zehn Jahre Aufbewahrungspflicht), für das Patientendossier zusätzlich im ePatientendosier-Gesetz. Ein entsprechender Verweis für die Regelungen im Gesundheitswesen könnte angezeigt sein.
IG eHealth	DSG	4	6		Der Artikel ist auf das Gesundheitswesen anzupassen oder sollte ersatzlos gestrichen werden.
IG eHealth	DSG	5			Die Voraussetzungen für den länderübergreifenden Datenaustausch sind viel zu komplex und müssen vereinfacht werden, damit sie praktikabel sind. Auch die Regeln für das ePatientendossier müssen festgelegt werden.
IG eHealth	DSG	8			Der EDOEB soll gemäss dem Gesetzesentwurf Empfehlungen der guten Praxis festlegen. Dies ist aus rechtsstaatlichen Gründen abzulehnen, auch wenn die Regeln nicht bindend sind.
IG eHealth	DSG	12			Der Artikel ist auf das Gesundheitswesen anzupassen oder sollte ersatzlos gestrichen werden. Es darf nicht sein, dass ein ganzes ePatientendossier an Nahestehende geht, ohne dass der Nachweis eines schützenswürdigen Interessens erbracht werden muss.
IG eHealth	DSG	13	3 und 4		Die Im ePatientendossier-Gesetz geregelte Informationspflicht (inkl. der Ausnahmen) ist im DSG zu berücksichtigen.
IG eHealth	DSG	13			Die Pflichten sollen nicht über die Vorgaben im EU-Recht hinausgehen.
IG eHealth	DSG	19			Die Pflichten sollen nicht über die Vorgaben im EU-Recht hinausgehen.

IG eHealth	DSG	8	50 bis 55		Die Strafbestimmungen müssen im Hinblick auf mögliche Gerichtsverfahren konkreter formuliert werden. Die Strafbestimmungen müssen in Einklang mit dem Arztgeheimnis (Art. 321 StGB) gebracht werden. Die Fahrlässigkeit soll gemäss OR festgelegt werden.
IG eHealth	DSG				
Fehler! erweisquelle konnte nicht gefunden werden.					
Fehler! erweisquelle konnte nicht gefunden werden.					
Fehler! erweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	
Fehler! erweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"		
Name/Firma	**Art.**	**Bemerkung/Anregung**
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		
Fehler! erweisquelle konnte nicht gefunden werden.		

IGE | IPI

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale
Swiss Federal Institute of Intellectual Property

Stauffacherstrasse 65/59 g | CH-3003 Bern
T +41 31 377 77 77
F +41 31 377 77 78
info@ipi.ch | www.ige.ch

Abteilung Recht & Internationales

A-Post
Bundesamt für Justiz
z.H. Herr Jonas Amstutz
Bundesrain 20
3003 Bern

Bern, 31. März 2017

Direktwahl +41 31 377 72 36
E-Mail: evelyne.keller@ipi.ch

Antrag im Vernehmlassungsverfahren zur DSG-Revision

Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Gerne nutzen wir die Gelegenheit, im Rahmen des Vernehmlassungsverfahrens zur Revision des Datenschutzgesetzes Stellung zu nehmen. Wir begrüssen die geplante DSG-Revision dem Grundsatz nach, erlauben uns aber nachfolgende Bemerkungen zum erweiterten Anwendungsbereich des DSG:

Der Vorentwurf sieht vor, die Ausnahmen betreffend öffentliche Register des Privatrechts aufzuheben (aktuell Art. 2 Abs. 2 lit. d DSG). Die Aufhebung dieser Ausnahme betrifft auch die IP-Register, worunter – nebst dem im Botschaftsentwurf ausdrücklich erwähnten Markenregister – auch das Patent- und das Designregister fallen. Das Eidgenössische Institut für Geistiges Eigentum (IGE) ist als Kompetenzzentrum des Bundes für Immaterialgüterrecht und insbesondere als registerführende Behörde von einer solchen Änderung besonders betroffen.

Es entspricht einem grundlegenden, weitherum akzeptierten und bewährten Prinzip im Bereich des geistigen Eigentums, dass die „Gegenleistung" für die Gewährung eines staatlichen Ausschliesslichkeitsrechts in der Publikation des Schutzrechts und den zugehörigen Angaben besteht. Diese Angaben (namentlich zur Inhaberschaft des Rechts) sind zentral für die anderen Wettbewerbsteilnehmer, die wissen müssen, welche Rechte bestehen, wie weit sie reichen und wem sie gehören. Der Gesetzgeber hat deshalb die Abwägung zwischen den Interessen der Öffentlichkeit an einer Offenlegung und denjenigen der Rechtsinhaber an einer Geheimhaltung bereits sorgfältig vorgenommen. Entsprechend enthalten die Bestimmungen in den immaterialgüterrechtlichen Spezialgesetzen eine klare und transparente Regelung, welche Angaben im Register publiziert und offenzulegen sind. Für eine Interessenabwägung unter dem Gesichtspunkt des Datenschutzrechts bleibt deshalb kein Raum: Die Einsicht ins Register und in die Akten von Rechten des geistigen Eigentums sind in den Spezialgesetzen eingehend geregelt. Insbesondere enthalten die Bestimmungen für die Akteneinsicht auch Ausnahmen, bei denen auf Antrag des Rechtsinhabers sensitive Dokumente ausgesondert werden können (vgl. Art. 36 Abs. 3 MSchV, Art. 22 Abs. 2 DesV, Art. 38 Abs. 4 PatV sowie Art. 90 Abs. 5 PatV). Damit besteht in unseren Augen kein Raum mehr für eine Prüfung schützenswerter Interessen von betroffenen Personen im Rahmen des DSG. Eine solche würde im Gegenteil Gefahr laufen, widersprüchliche Wertungen bei der Beurteilung der Einsicht einzuführen. Dies insbesondere auch vor dem Hintergrund, dass es sich bei den in den IP-Registern publizierten Personendaten nicht um besonders schützenswerte Daten im Sinn des DSG handelt. Die Ausnahme betreffend IP-Register stellt sicher, dass die Rechtsanwendung im Bereich des geistigen Eigentums übersichtlich und praktikabel bleibt. Das entspricht auch internationalen Standards im Bereich des Immaterialgüterrechts.

Eine Unterstellung der IP-Register unter den Anwendungsbereich des DSG wäre für die betroffenen Schutzrechtsinhaber und IP-Spezialisten mit grossen Rechtsunsicherheiten verbunden. Insbesondere könnte das IGE aufgrund der allenfalls im Einzelfall vorzunehmenden Interessenabwägung nicht mehr gewährleisten, dass die unter der Onlineplattform www.swissreg.ch publizierten Daten mit denjenigen der Register übereinstimmen. Damit würde das Recht auf Öffentlichkeit der Rechte an geistigem Eigentum und das grundlegende Prinzip im Immaterialgüterrecht – staatliches Ausschliesslichkeitsrecht gegen Offenlegung der Inhaberschaft – ausgehebelt.

Aus diesen Gründen stellt das Eidgenössische Institut für Geistiges Eigentum folgende Anträge:

1. **Art. 2 Abs. 2 des revidierten Datenschutzgesetzes sei wie folgt zu ergänzen:**

   „e. öffentliche Register des Immaterialgüterrechts."

2. **In der Botschaft zum revidierten Datenschutzgesetz sei ausdrücklich darauf hinzuweisen, dass der Gesetzgeber im Bereich der IP-Register die Interessenabwägung bereits vorgenommen hat und der Publizität der Register und sonstigen öffentlich zugänglichen Daten den Vorrang gegenüber anderweitigen Interessen gewährt hat.**

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und für die Berücksichtigung unseres Anliegens. Für Rückfragen, sei es telefonisch oder im Rahmen eines persönlichen Gesprächs, stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

E. Keller

Evelyne Keller
Rechtsdienst Allgemeines Recht, Designs und Rechtsdurchsetzung

IGEM, c/o Ueli Custer, Erlenweg 13, CH-4524 Lommiswil

Per E-Mail an jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 4. April 2017

Stellungahme der IGEM zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die IGEM vereinigt die Anbieter und Abnehmer von Werbezeiten in elektronischen Medien und im Internet und setzt sich für liberale gesetzliche Rahmenbedingungen ein. Mitglieder sind sowohl praktisch alle relevanten Mediaagenturen sowie die Vermarktungsfirmen von elektronischer und digitaler Werbung in TV, Radio Kino und Online aber auch die für die Branche wichtigen Marktforschungsunternehmen. Sie setzt sich insbesondere für vielfältige und liberale Möglichkeiten der kommerziellen Kommunikation in diesen Medien ein. Wir erlauben uns deshalb, Ihnen eine kurze Stellungnahme zukommen zu lassen.

Besonders wichtig ist aus Sicht der IGEM, dass mit dem Gesetz die durch den Bundesrat am 17. Januar 2017 verabschiedeten Rahmenbedingungen der digitalen Wirtschaft nicht unterlaufen werden. Dies ganz speziell im Hinblick auf die Aussage **„Der digitale Wandel bietet grosse Chancen für die Schweizer Volkswirtschaft. Der Bundesrat will diese nutzen, um Arbeitsplätze und Wohlstand zu sichern."**

Wenn nun aber wie im vorliegenden Entwurf die Regelungen teilweise weit über das in der EU geltende Recht hinaus die schweizerische Kommunikationswirtschaft einschränken, widerspricht dies eindeutig diesen Vorgaben. **Auf Regelungen, die weiter gehen als das EU-Recht ist deshalb konsequent zu verzichten.** Denn diese führen zu einem Standortnachteil für Unternehmen, die in der Schweiz ansässig sind.

Ganz speziell möchten wir dabei auf die unverhältnismässig hohen Anforderungen an das zu wenig klar definierte Profiling verweisen. Hier ist strikte darauf zu achten, dass die Regelungen nicht für Anwendungen mit nicht personengebundenen Daten gelten. **Die im Entwurf vorgeschlagene Definition des Profiling geht weit über diejenige der EU-DSGVO hinaus** und führt dadurch ebenfalls zu einem Standortnachteil für Unternehmen in der Schweiz.

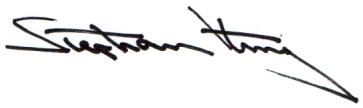
Im Übrigen verweisen wir auf die Stellungnahmen von KS/CS (Kommunikation Schweiz), des Interactive Advertising Bureau (IAB) Switzerland sowie des SDV (Schweizer Dialogmarketing Verband) denen wir uns weitgehend anschliessen. Dies betrifft insbesondere die Forderung von KS/CS, **das Datenschutzgesetz nur insoweit zu revidieren, als dies die internationalen Vorgaben zwingend erfordern.** Jeder darüber hinausgehender „Swiss Finish" ist strikte abzulehnen**.**

IGEM · Interessengemeinschaft elektronische Medien, UID: CHE-153.928.450
c/o Ueli Custer · Erlenweg 13 · CH-4514 Lommiswil
T +41 32 641 06 10 · F +41 32 641 34 86 · info@igem.ch · www.igem.ch

Wir danken Ihnen für die Kenntnisnahme.

Freundliche Grüsse

IGEM



Stephan Küng
Präsident

Ueli Custer
Geschäftsführer

IGEM · Interessengemeinschaft elektronische Medien, UID: CHE-153.928.450
c/o Ueli Custer · Erlenweg 13 · CH-4514 Lommiswil
T +41 32 641 06 10 · F +41 32 641 34 86 · info@igem.ch · www.igem.ch

Amstutz Jonas BJ

Von: Kurt Weigelt <kurt.weigelt@ihk.ch>
Gesendet: Mittwoch, 22. März 2017 10:05
An: Amstutz Jonas BJ
Betreff: DSG, Stellungnahme
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de.docx

Sehr geehrter Herr Amstutz

Im Anhang die Stellungnahme der IHK St.Gallen-Appenzell zum Vorentwurf DSG.

Freundliche Grüsse
Kurt Weigelt

IHK St.Gallen - Appenzell
Dr. Kurt Weigelt, Direktor
Gallusstr. 16, Postfach
CH - 9001 St.Gallen
Tel. 071 224 10 12
kurt.weigelt@ihk.ch
www.ihk.ch / www.kurtweigelt.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Industrie- und Handelskammer St.Gallen-Appenzell

Abkürzung der Firma / Organisation : IHK

Adresse : Gallusstrasse 16

Kontaktperson : Dr. Kurt Weigelt

Telefon : 071 224 10 12

E-Mail : kurt.weigelt@ihk.ch

Datum : 22.3.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
IHK	Die IHK St.Gallen-Appenzell vertritt 1600 Ostschweizer Unternehmen mit rund 90'000 Mitarbeitenden. Zwei Drittel unserer Mitgliedunternehmen beschäftigen weniger als 50, ein Drittel weniger als 50 Mitarbeitende. Unsere Stellungnahme orientiert sich daher insbesondere an den Bedürfnissen kleinerer und mittlerer Unternehmen.
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG				Vorbemerkung: Der Vorentwurf zum DSG zeugt insgesamt von einem ausgeprägten bürokratischen Übereifer. Die vorgeschlagenen Regelungen sind aus Sicht von Unternehmen ohne eigene Rechtsabteilung nicht praktikabel. Einmal mehr entsteht der Eindruck, dass die Bundesverwaltung jeden Bezug zu den Realitäten kleinerer und mittlerer Unternehmen verloren hat.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	1			Nicht nur die juristischen Personen, sondern auch die im HR eingetragenen Einzelunternehmen und Mitglieder von Personengesellschaften sind vom Schutz auszunehmen. Die Abgrenzung der geschützten von den nicht geschützten Personenkategorien ist in dieser Form nicht sachgerecht. Im HR eingetragene Einzelfirmen oder Mitglieder von Personengesellschaften sind gleich zu behandeln wie juristische Personen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	2	Abs. 2	lit. c	Beibehaltung des geltenden Wortlauts. Der VE will nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung also nicht mehr gelten. Dies öffnet Missbräuchen Tür und Tor (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben wer-den müsste, etc.).
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	3	lit.c	Ziff. 4	Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Bilder in Zeitungen wären damit ausgenommen (nachjetzigen dem Wortlaut würden sie unter den Begriff der "biometrischen Daten" fallen).

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3	lit. c	Ziff. 5	Die Bestimmung ist in dieser allgemeinen Form problematisch. etwa wenn Vermögensdelikte zur Diskussion stehen, von denen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	3	lit. f		Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes "Daten". Letzteres ist überflüssig und irrführend; es geht im DSG immer nur um "Personendaten". Die reflexartige Übernahme von Begriffen des ausländischen Rechts beinhaltet die Gefahr, dass auch die Anwendung sich primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und weder notwendig noch sachgerecht. Dies umso weniger, als der Begriff des "Profiling" gegenüber dem EU-Recht sogar ausgeweitet worden ist; die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bea-beitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Kautelen und Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Was damit gewonnen wäre, ist unerfindlich. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich höchst kontraproduktiv, die Bearbeitung solcher Informationen nur deswegen zu erschwe-ren, weil sie theoretisch als "Voraussage" eines späteren Verhaltens interpretiert werden können. Die Revision schiesst hier weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen. ohne all die Kautelen einzuhalten, die der VE mit dem "Profiling" verknüpft; selbst die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind, würde plötzlich problematisch, etc.

					Der Begriff des "Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem "Persönlichkeits-profil" des geltenden Rechts absolut abzulehnen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	3	lit. h lit. i		Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), eventualiter zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu unklaren - teilweise unsinnigen - Aufteilungen der Verantwortung und Doppelspurigkeiten. Offenbar wird zudem übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen kann. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für den "Verantwortlichen"?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den "Verantwortlichen?") geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den "Verantwortlichen"?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht- Unklar ist auch, ob Arbeitnehmer unter den Begriff des "Auftragsbearbeiters" fallen können, was dem Wortlaut und der Systematik entspräche, aber offensichtlich zu einer völlig ausufernden Verantwortlichkeit führen würde.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	4	Abs. 3		Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft nur neue Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Vorausset-zungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Die Botschaft argumentiert, es sei keine Änderung beabsichtigt. Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. Die Einführung kompatibler Bearbeitungszwecke ist zu begrüssen.
Fehler! Verweisquelle konnte nicht	DSG	4	Abs. 4		Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.

gefunden werden.IHK					
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	4	Abs. 5		Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Seite 47 des Erläuterungs-berichts sind hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten, sonst wird nur neue Unsicherheit geschaffen. Eventualiter: Beschränkung von Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind", Streichung des Restes dieses Passus'. Bekanntlich fängt die "Bearbeitung" ja schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE). Eine fortdauernde Verpflichtung zur Nachführung wäre offensichtlich unerfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status' einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind!
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	4	Abs. 6		Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (s. auch die Bemerkungen zu Art. 3 lit. f VE)
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	5	Abs. 3	lit. d	Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	5	Abs. 4 bis 6		Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt - wie aus dem Wort ersichtlich - nach den Weisungen des Verantwortlichen, dem - wiederum entsprechend seiner Bezeichnung - die Verantwortung für die Information des Beauftragten obliegt.
Fehler! Verweisquelle konnte nicht	DSG	6	Abs. 2		Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1, lit b, c und d ins Ausland bekanntgegeben wird; dies gilt erst

gefunden werden.IHK					recht, wenn - wie hier - neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Die Verantwortlichkeiten sind einmal mehr unklar geregelt. Die Bestimmung ist im Übrigen auch insofern heikel, als solche Meldungen z.T. sensible Geschäftsinterna betreffen werden (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetz auch für Dritte einsehbar werden. Dem Schutz von Geschäftsgeheimnissen ist im Rahmen des VE DSG generell nicht die nötige Aufmerksamkeit geschenkt worden.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	7	Abs. 2		Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftrags-bearbeiters zu präzisieren. Der Auftragsbearbeiter ist auch hier zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	7	Abs. 3		Schaffung der Möglichkeit einer generellen Einwilligung.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	8			Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der "interessierten Kreise" - erfahrungsgemäss damit einseitig der politischen Linken - ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. U.a. ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen tel quel zugrunde legen werden. Der Beauftragte wird im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich Recht zu setzen. Dies wiegt umso schwerer, als der Beauftragte noch nicht einmal Jurist zu sein braucht.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	9			Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zulasten des Datenbearbeiters führen.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	12	Abs. 4		Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Allfällige Änderungen wären im ZGB vorzunehmen. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichti-gungs- und Löschungsrecht völlig ausreichen. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären, etc-. Art. 4 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegen-stehen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	13			Vorbemerkungen: Es fehlt an Übergangsbestimmungen, die regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar. Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich angemessenen" Datenschutz zu liefern haben.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	13	Abs. 1 und 2		Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird festgehalten, es genüge eine "allgemeine Information" im beschriebenen Sinn (vgl. S. 55). Der Wortlaut von Art. 13 VE widerspricht dem allerdings. In der vorliegenden Form ist die Bestimmung völlig unpraktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen

					sie alle informieren, deren Daten sie bearbeiten. In einem Wort: Ein kompletter Overkill (dies wurde sogar in der RFA der PWC richtig er-kannt, wenn auch anscheinend nur von einer Minderheit; vgl. Ziff. 4.1.1.5 des genannten Dokuments). Dieser wäre umso gravierender, als dann je nach Tätigkeit des datenverarbeitenden Unternehmens jedermann auch noch sämtliche Empfänger und Empfängerinnen bekanntgegeben - und damit Geschäftsgeheimnisse offenge-legt - werden müssten. Der Aufwand wäre schlicht jenseits von Gut und Böse. Es muss genügen, dass diese Informationen öffentlich zugänglich sind.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	13	Abs. 3		Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist unakzeptabel. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungs-pflicht wäre in jedem Fall auf solche Fälle zu beschränken, wo persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswir-kungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger auch noch der "unschuldigsten" Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen. Bemerkung: Die Weitergabe von Daten innerhalb eines Konzerns wird damit unnötig erschwert (Konzerngesellschaften gelten ja als Dritte)
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	13	Abs. 4		Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	13	Abs. 5		Ersatzlos streichen; eventualiter. Beschränkung der aktiven Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten. Die vorliegend stipulierte, uferlose Informationspflicht ist impraktikabel und völlig unverhältnismässig. Die Bestimmung ist im Übrigen strenger als die DSGVO, die immerhin noch einen Monat Frist gewährt (!). Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es

					muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	14			Vorbemerkung: Wurde unnötigerweise enger als die CON108 gefasst
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	14	Abs. 1		Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung), in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	14	Abs. 2		Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Infor-mationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der Vorentwurf für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	14	Abs. 4	lit. a	Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Bemerkung: Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns unnötig erschwert.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	15	Abs. 1		Streichen, ev. um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a) DSGVO EU (2016/679) ergänzen; weiter wäre ausdrücklich vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als überzogener und unreflektierter Versuch, Konsumenten vor jedweder Art von automatisierten Entscheidungen zu "schützen", die sich

					irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche Auswirkung ist, dürfte letztlich von der Sensibilität des Betroffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte Art. 22 DSGVO EU nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor - eine Abweichung wäre demnach zweifellos auch für die Schweiz zulässig. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Die Formulierung der "Auswirkungen" ist so breit, dass jeder kommerzielle Entscheid - z.B. über eine Lieferung von Ware gegen Rechnung - darunter fallen kann. Auch die Lieferung von Ware gegen Rechnung ist in keiner Weise zwingend, und die Verweigerung darf nicht begründungspflichtig werden.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	15	Abs. 2		Streichen; wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand. Jedes Unternehmen, das über ein strukturiertes Kreditmanagementsystem verfügt, wird inskünftig mit jedem, den es nicht gegen Rechnung beliefern will, Korrespondenz führen müssen um ihm zu erklären, wie der Entscheid zustan-de gekommen ist. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens. Es scheint den Autoren des VE entgangen zu sein, dass in der Schweiz grundsätzlich immer noch Vertragsfreiheit herrscht, und niemand sich für seine Lieferkonditionen rechtfertigen muss. Der VE geht, wie erwähnt, in diesem Punkt sogar über die DSGVO hinaus.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	15	Abs. 3		Streichen. Diese Bestimmung entlastet einmal mehr einseitig den Staat.

Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	16			Antrag: Streichen. In den Wortlaut kann jeder hineindeuten, was er will. Im Ergebnis wird wohl jedes Unternehmen eine solche "Folgeabschätzung" vornehmen müssen, welches mehr tut, als die Daten seiner eigenen Kunden zu bearbeiten. Hier wird ein bürokratisches Monstrum in die Welt gesetzt, das in der Privatwirtschaft im Ergeb-nis nichts bringen wird (im öffentlichen Sektor mag es hingegen durchaus ange-bracht sein). Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier und Zeit dafür aufwenden müssen. Der Verweis auf die Grundrechte macht übrigens einmal mehr deutlich, dass ein Datenschutzgesetz, welches sowohl den privaten als auch den öffentlichen Sektor regeln will, zwangsläufig zu Regulierungen führt, die dem einen oder anderen Bereich unangemessen sind. Vor kurzem war der Tagespresse zu entnehmen, wie schwer der Bundesrat sich mit der Aufgabe der Regulierungsfolgeabschätzung tut. Dies sollte auch hier zur Vo-sicht mahnen; im Gegensatz zu staatlichen Organen hat ein Rechtsunterworfener ja gravierende Konsequenzen bis hin zu seiner wirtschaftlichen Vernichtung zu befürchten für den Fall, dass er die Aufgabe der "Folgenabschätzung" nicht zur Zufriedenheit der Amtsstellen oder Gerichte löst, die sich mit ihm befassen wollen oder müssen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	16	Abs. 3 und 4		Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist wäre im Übrigen auch zu lang.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	17			Antrag: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechts-system völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien. Wieso dieser im Bereich des Datenschutzes plötzlich nicht mehr gelten soll,

					ist völlig unerfindlich; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Der Verantwortliche müsste sich m.a.W. nicht nur an das datenschutzrechtliche, sondern auch noch an das strafrechtliche Messer liefern. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der nachgerade terroristischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer regelrechten Flut an Selbstanzeigen zu rechnen, die nur den Apparat des Beauftragten übermässig aufblähen würde.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	17	Abs. 2		In jedem Fall Streichung des Rechts des Beauftragten, die Information des Be-troffenen zu verfügen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	17	Abs. 4		Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	18			Antrag: Streichen. Die Bestimmung ist redundant, der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Fehler! Verweisquelle konnte nicht	DSG	19			Antrag: Streichen. Die Bestimmung ist nicht nur überflüssig, sondern teilweise gar nicht umsetzbar.

gefunden werden.IHK					Die stipulierte Dokumentationspflicht würde für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b. ist sodann von vornherein nicht umsetzbar bzw. nachgerade absurd. Was gewonnen sein soll, wenn alle früheren Empfänger von Daten über jede spätere Änderung, Löschung oder Vernichtung informiert werden, ist völlig unerfindlich. Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine - allfällige - Verletzung von Datenschutzgrundsätzen machen zu müssen oder über "Einschränkungen" der Datenbearbeitung gem. Art. 25 machen zu müssen (bei der obendrein nicht klar ist, was man sich darunter vorzustellen hätte). Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Zudem würde die Umsetzung der Bestimmung häufig ihrerseits zu Datenschutzverletzungen führen. Bezüger von Wirtschaftsauskünften haben häufig gar kein schützenswertes Interesse daran, von späteren Änderungen einer Auskunft Kenntnis zu erhalten; dies gilt z.B. immer dann wo die vertraglichen Beziehungen zum Betroffenen fertig abgewickelt sind. Sie über spätere Berichtigungen zu informieren, würde zweifellos einen Verstoss gegen das DSG bedeuten.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	20	Abs. 2	lit. e	Antrag: Streichen - in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich, z.B. im Online-Handel, etc. Vgl. auch den Antrag zu Art. 15 hievor.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	20	Abs. 2	lit.f	Antrag: Streichen: Die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntzugeben, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	Abs. 3		Antrag: Streichen, ev. Beschränkung auf die Pflicht, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt - ein Vertrag wird geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, Geschäftsgeheimnisse offenlegen zu müssen, die ansonsten ausdrücklich strafrechtlich geschützt sind. Wieso es erforderlich sein soll, dem Betroffenen die Auswirkungen zu erläutern, ist sodann völlig unerfindlich. In aller Regel wird er absolut in der Lage sein, diese selber einzuschätzen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	23	Abs. 2	lit. d	Antrag: Streichen. Zum Profiling vgl. auch die Bemerkungen zu Art. 3 lit. f) VE.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	23	Abs. 3		Abs. 3 gaukelt eine scheinbare Sicherheit vor. Was über Facebook verbreitet worden ist, kann auch dann nicht wieder aus der Welt geschafft werden, wenn der Betroffene Facebook die (weitere) Verbreitung untersagt
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	24	Abs. 2		Erster Satz: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. Das neue DSG wimmelt nachgerade von Vorschriften, die einseitig auf die Einschränkung der Datenbearbeitung und auf eine Kriminalisierung datenbearbeitender Unternehmen ausgerichtet sind.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	24	Abs. 2	lit. a	Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft einmal mehr nicht gelöste Abgrenzungsfragen auf.

Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	24	Abs. 2	lit.c Ziff.3	Antrag: Steichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar, die Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft. Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit 100 %-iger Sicherheit bestimmbar, geschweige denn sein Alter. Im Übrigen würde es klar zum Schutz Minderjähriger beitragen, wenn zumindest ihr Alter gespeichert und die Information aufbewahrt werden dürfte!
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	25	Abs. 1	lit. a) bis c)	Müsste spezifiziert werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. ansonsten kann die Bestimmung nicht umgesetzt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	25	Abs. 2		Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", ev. Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich um bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis krause Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	25	Abs. 3		Abs. 3. streichen. lit. a bis c reichen völlig, um dem Betroffenen Genüge zu tun.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	28	Abs. 1 und 2		Entweder streichen, oder die entsprechenden Möglichkeiten auch Privaten eröffnen. Hier kommt einmal mehr das einseitig etatistische Denken zum Ausdruck, das dem ganzen Erlass zugrunde liegt.

Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	37	Abs. 1		Dem Bundesrat soll nur ein Vorschlagsrecht zukommen, die Wahl muss durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Dauer von 4 Jahren gewählt". Ein blosses Recht des Parlaments, den Gewählten abzunicken, ist als Augenwischerei zurückzuweisen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	37	Abs. 4		Das Budget muss durch das Parlament genehmigt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	38	Abs. 2		Die automatische Wiederwahl ist zu streichen. Ein solches Institut existiert bei keiner anderen, magistralen Position.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	39	Abs. 2		Jede Nebenbeschäftigung muss offengelegt werden. Hier ist absolute Transparenz unabdingbar.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	41	Abs. 4		Antrag: Streichen. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne konkrete Hinweise auf eine Datenschutzverletzung ist strikte abzulehnen. Die Kosten solcher amtlicher Initiativen werden in der Praxis regelmässig den Privaten überbunden. Daher muss gelten: Keine "Überprüfung" ohne konkreten Anlass!
Fehler! Verweisquelle konnte nicht	DSG	42			Antrag:

gefunden werden.IHK					Streichen. Vorsorgliche Massnahmen sind - auch im Persönlichkeitsschutz - Sache der Gerichte. Hier soll einer Einzelperson, die nicht einmal Jurist sein muss, ohne Not eine völlige "carte blanche" erteilt werden! Dies ist rechtsstaatlich unhaltbar.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	43	Abs. 1		Antrag: Streichen. Der Beauftragte erhält hier Befugnisse zum Erlass hoheitlicher Verfü-gungen, die teilweise nicht wieder gutzumachende Folgen zeitigen (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungs-pflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 42 reicht zum Schutz Betroffener völlig aus.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	44	Abs. 3		Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Wenn schon, wäre vorzusehen, dass die aufschiebende Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt unsinnige Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	45			Antrag: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	49		lit.b	Antrag: Streichen. Es besteht die Gefahr, dass der Beauftragte zum verlängerten Arm ausländischer Behörden wird.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	50			Das gesamte Sanktionensystem (Art. 50 ff.) ist zu überarbeiten. U.a. sind - wenn schon - bei Verstössen grundsätzlich Verwaltungsbussen vorzusehen und nicht strafrichterliche Verurteilungen. Der vorgesehene Strafrahmen ist sodann nachgerade als terroristisch zu bezeichnen. Dies gilt sowohl für vorsätzliche als auch - erst recht - für fahrlässige Verstösse. Es wird beantragt, bei

					Fahrlässigkeit von einer strafrechtlichen Sanktionierung abzusehen, eventuell den Bussenrahmen auf eine maximale Höhe von CHF 5'000.00 bzw. - im Wiederholungsfall - CHF 10'000.00 zu begrenzen. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO EU bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 lit. geht von 2 % des weltweiten Umsatzes eins Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen; die Umsatzrendite beträgt bei hiesigen KMU häufig weniger als 5 %). Die Strafbestimmungen stellen ein weiteres Beispiel dar, wie sehr der Politik das Augenmass abhandengekommen ist. Offenbar hat sich inzwischen der Glaube durchgesetzt, dass ein Gesetz nur dann ein gutes sein kann, wenn es Strafdrohungen im Phantasiebereich enthält und möglichst viele Akteure kriminalisiert. Theoretisch genügt EIN Betroffener, der sich falsch behandelt fühlt, um einen Datenbearbeiter als Kriminellen abzustempeln und wirtschaftlich in den Ruin zu treiben. Im "gewöhnlichen" Strafrecht beträgt die maximale Busse für eine Übertretung CHF 10'000.00 (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Rahmen. Die Erhöhung des Strafrahmens auf CHF 500‘000.00 ist völlig überrissen. Beispielsweise sieht das kantonalbernische Verwaltungsrecht im Baurecht bei schweren (!) Verstössen Höchstbussen von CHF 100'000.00 vor (Art. 50 Abs. 3). Gemäss Art. 14ff. VStrR können bei Leistungs- und Abgabebetrug, Urkundenfälschung und Erschleichung einer Falschbeurkundung sowie Begünstigung Höchstbussen von CHF 30'000.00 festgelegt werden. Gemäss DBStG können bei Verstössen wie Mithilfe bei der Steuerhinterziehung Bussen von 10‘000.00 bis max. CHF 50‘000.00 (in schweren Fällen oder bei Wiederholungsfall) gesprochen werden. Bei Steuerbetrug beträgt die Busse max. 30‘000.00. Bei Verstössen gegen das DSG handelt es sich mi Ausnahme von Art. 52 VE - der eine Freiheitsstrafe als Höchststrafe vorsieht - nicht um Vergehen oder Verbrechen, sondern um Uebertretungen. Es existiert kein nachvollziehbarer Grund, für vergleichbare Verstösse übliche

					Bussenrahmen im DSG um das Zehnfache oder mehr zu überschreiten. Eine Persönlichkeitsverletzung, die dies rechtfertigen würde, ist nicht vorstellbar. Eine solche Pönalisierung von DSG-Verstössen kommt einer schweren Kriminalisierung der Fehlbaren gleich und ist komplett unverhältnismässig. U.a. übersteigt der im VE DSG gesteckte Rahmen auch Schmerzensgelder bei weitem, die nach hiesiger Rechtsprechung bei Körperschäden zugesprochen werden. Als Vergleich noch einige Beispiele aus der deutschen Rechtsprechung für die Bemessung von Schmerzensgeld wegen Persönlichkeitsverletzung (Mobbing und ähnliches): ▪ Mobbing durch nicht gerechtfertigte Aufgabenentziehung durch den Arbeitgeber, Schikanierung und Degradierung des Arbeitnehmers: 53.000 Euro (ArbG Leipzig, 2012) ▪ vielfältige persönliche Herabsetzung des Arbeitnehmers, rund € 26.500, ArbG Ludwigshafen am Rhein, 2000 ▪ Beleidigungen, Auftragsentziehung, Verbot des Kundenkontakts, Gehaltskürzung durch den Arbeitgeber, € 24.000 , LAG Hannover, 2005 ▪ systematische Persönlichkeitsverletzungen des Arbeitnehmers in 34 Fällen über 1 Jahr, € 17.500, ArbG Eisenach, 2005 ▪ schikanöse und entwürdigende Handlungen, € 7.000, ArbG Siegburg, 2012 ▪ Demütigung wegen der ethnischen Herkunft durch ein Rap-Video bei YouTube, € 5.000, LG Bonn, 2013 ▪ Cybermobbing via Facebook mit Unterstellung der Homosexualität und Pädophilie, € 1.500, LG Memmingen, 2015 Quelle: http://www.schmerzensgeldtabelle.net/mobbing/#tabelle
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	51	Abs. 2		Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen. Vorsatzstrafen: S. Bemerkungen zu Art. 50

Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	52			Antrag: Streichen. Die strafrechtlichen Bestimmungen über die berufliche Schweige-pflicht sind völlig ausreichend. Unklar, wer hier neu zum Träger eines Berufsgeheimnisses gemacht werden soll, ebenso unklar, was "geheime Personendaten" im vorliegenden Zusammenhang genau bedeuten würde. Wenn schon die blosse kommerzielle Bearbeitung von Daten als Aufhänger für die Strafdrohung genügen, würde wohl nahezu jeder Datenbearbeiter zum Träger einer strafbewehrten Schweigepflicht gemacht.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	54			Antrag: Streichen. Die Verfahren sind auf dem Verwaltungsweg und somit vom Bund zu führen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DSG	55			Reduktion der Verjährungsfrist auf 3 Jahre. Dies entspricht Art. 109 StGB und wäre völlig ausreichend und sachgerecht (auch im Verwaltungsverfahren)
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	DGS	56			Die Genehmigung des Parlamentes ist zwingend einzuholen.
Fehler! Verweisquelle konnte nicht gefunden werden.IHK	ZPO	20 99 113 114	 Abs. 3 Abs. 2	Bst. d Bst. d Bst. d Bst. f	Antrag: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Wo das Gesetz in Abweichung von den normalen Regeln von der Erhebung von Gerichtskosten absieht, geht es üblicherweise um Vertragsstreitigkeiten (Miete, Arbeitsvertrag, auch

		243	Abs. 2	Bst. d	Gleichstellungsfragen pflegen sich jeweils im Zusammen-hang mit einem Arbeitsverhältnis zu stellen). Wegleitend ist dabei die Annahme des Gesetzgebers, dass eine Partei besonders geschützt werden muss, weil sie in einem Abhängigkeitsverhältnis zur anderen steht. Im Datenschutzbereich werden oft keinerlei vertragliche oder persönliche Beziehungen zwischen Datenbearbeiter und Betroffenem bestehen. In dieser Konstellation ist nachgerade mit einer Flut von - durchaus auch mutwilligen - Klagen zu rechnen, wenn das Prozessieren gratis ist. Es besteht kein Anlass, die üblichen, zivilprozessualen Regeln hier zu ändern. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll - wie dies bei zivilrechtlichen Streitigkeiten grund-sätzlich der Fall ist - seine Kostenrisiken abwägen müssen. Der SVC spricht sich auch dagegen aus, alle Streitigkeiten ins vereinfachte Ver-ahren zu weisen. Dies verkürzt die beklagte Partei wesentlich in ihren Verfahrensrechten.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		

Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Amstutz Jonas BJ

Von: Adrian Derungs <Adrian.Derungs@ihz.ch>
Gesendet: Donnerstag, 30. März 2017 15:33
An: Amstutz Jonas BJ
Cc: Felix Howald
Betreff: Stellungnahme Vernehmlassung Revision Datenschutzgesetz (DSG)
Anlagen: Vernehmlassung_Datenschutzgesetz_IHZ.docx

Sehr geehrter Herr Amstutz,

Im Anhang übermittle ich Ihnen die Vernehmlassungsantwort der Industrie- und Handelskammer Zentralschweiz (IHZ) zur Revision des Datenschutzgesetzes (DSG). Die IHZ vertritt als Wirtschaftsverband über 700 Unternehmen in der Zentralschweiz.

Da sich unsere Stellungnahme zu grundsätzlichen Aspekten der Revision äussert, haben wir auf die Benutzung des elektronischen Formulars verzichtet; wir danken für Ihr Verständnis. Für eine kurze Bestätigung über den Erhalt der Vernehmlassung danke ich Ihnen im Voraus.

Besten Dank für die Berücksichtigung unserer Stellungnahme. Für Rückfragen stehe ich gerne zur Verfügung.

Freundliche Grüsse

Adrian Derungs

IHZ Industrie- und Handelskammer Zentralschweiz
Adrian Derungs
Wirtschaftspolitischer Mitarbeiter
Kapellplatz 2
Postfach
6002 Luzern

Tel. +41 (0)41 417 0146
Fax +41 (0)41 410 5288
adrian.derungs@ihz.ch
www.ihz.ch

Revision des eidgenössischen Datenschutzgesetzes (DSG)

Stellungnahme der Industrie- und Handelskammer Zentralschweiz (IHZ)

Die IHZ nimmt in summarischer Form zur Revisionsvorlage des DSG Stellung. In Bezug auf die einzelnen Bestimmungen und damit verbundenen Detailerläuterungen und Änderungsvorschlägen verweisen wir auf die Stellungnahme der economiesuisse, die wir unterstützen und welche die Grundlage bildet für die vorliegende, grundsätzliche Stellungnahme.

Die IHZ stellt fest, dass die Revision des DSG gemäss der durchgeführten Regulierungsfolgenabschätzung (RFA)[1] Nutzen generiert. Zentral ist dabei gemäss RFA die erhöhte Transparenz zugunsten der Datensubjekte im Verhältnis zu den datenverarbeitenden Akteuren. Auch der Erhalt des Status eines Staates mit adäquatem Datenschutz kann laut RFA mit der Revision abgesichert werden. Als weiteren Nutzen führt die Untersuchung die Kompetenzerweiterung der Datenschutzaufsichtsbehörde auf, womit die Durchsetzung des Datenschutzes in der Schweiz sowie das Bewusstsein der Wirtschaft und der Gesellschaft in Bezug auf den Datenschutz gestärkt werden sollen. Gleichzeitig steige so auch das Vertrauen der Datensubjekte gegenüber den Unternehmen und der Datenschutzaufsichtsbehörde.

Aus Sicht der Zentralschweizer Wirtschaft steht in Bezug auf den Nutzen der Revision v.a. im Vordergrund, dass man im internationalen Vergleich weiterhin einen angemessenen Datenschutz bietet und den entsprechenden Status absichern will. Dieses Ziel soll mit der Revision des DSG erreicht werden. Darüber hinausgehende Regulierungen sind hingegen weitgehend kontraproduktiv. Sie generieren keinen Nutzen, sondern führen zu gewichtigen Wettbewerbsnachteilen, die in der Folge knapp erläutert werden sollen:

- **Kostenfrage ungeklärt**: Grundsätzlich werden die Kosten für die Wirtschaft und die öffentliche Hand aufgrund der Umsetzung des geplanten DSG stark ansteigen. Für die Unternehmen resultiert aufgrund der Zunahme der Bearbeitungs- und Administrationsaufwandes für diverse Handlungspflichten massiver finanzieller Mehraufwand. Leider haben es die Verfasser der RFA verpasst, diese Mehraufwände in irgendeiner Form zu quantifizieren. Einmal mehr wird ein Gesetzesvorhaben somit zu einer Art „Blackbox“, die es weder dem Gesetzgeber noch den betroffenen Akteuren ermöglicht, die Kosten den Nutzen gegenüber zu stellen und die verschiedenen Interessen abzuwägen. Wir stehen dem vorliegenden Entwurf daher grundsätzlich kritisch gegenüber.

[1] https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Regulierung/regulierungsfolgenabschaetzung/vertiefte-rfa/datenschutzgesetz--dsg--2016/datenschutzgesetz-2016.html

- **Gesetzesflut führt zu Vertrauensverlust**: Wir zweifeln an der Haltung, wonach die Revision des DSG das Vertrauen der Datensubjekte in die Unternehmen steigere und dies letztlich zunehmend zur freiwilligen Übermittlung von Daten führen werde. Diese Haltung steht vielmehr für eine übertriebene paternalistische Einstellung, wonach der Staat besser als jeder Einzelne zu wissen glaubt, was für den Staatsbürger gut ist. Die Selbstverantwortung des Individuums erodiert so zunehmend, sie wird an die Gesetzgebung delegiert. Es wird der Eindruck vermittelt, dass Gesetzgebung grundsätzlich zu mehr Vertrauen führt. Im krassen Gegensatz zu dieser Haltung steht die Feststellung im Rahmen der RFA, dass bei den Unternehmen eine geringe Sensibilität besteht bezüglich der geltenden Datenschutzgesetzgebung. Wenn bereits die heute geltenden Vorgaben in Grossteilen der Bevölkerung und bei Unternehmen nicht bekannt ist, dann ist fragwürdig, wie neue und noch komplexere Regelungen an diesem Umstand etwas ändern sollen. Als Beispiel für diese gesetzgeberische Sackgasse sei auf die Finanzbranche verwiesen. Was in der Finanzbranche seit der Regulierungswelle in den vergangenen Jahren tatsächlich stark anstieg, sind v.a. die Compliance-Kosten. Diese stehen vermutlich in keinem günstigen Verhältnis zum Vertrauensgewinn im selben Zeitraum. Vertrauen wird nicht direkt durch strengere und komplexe gesetzliche Vorlagen zurückgewonnen, sondern durch die Handlungen der betroffenen Unternehmen. Dazu brauchen diese optimale Rahmenbedingungen, keine masslose Expansion der Regulierungen und damit verbundene Bürokratie und administrativer Aufwand. Dies gilt auch für den Datenschutz. In diesem heiklen Bereich soll der Gesetzgeber die Verschärfung von Regulierungen mit Bedacht wählen. Wie gross ist das tatsächliche Gefühl des Kontrollverlustes der eigenen Daten? Wie verhält sich dieser angebliche Kontrollverlust zu den bewussten Entscheiden einer Vielzahl von Nutzern, einen Grossteil persönlicher Daten verschiedenen Anbietern und Plattformen freiwillig preiszugeben? Ist dies tatsächlich ein paradoxes Verhalten oder nicht vielmehr Ausdruck einer selbstverantwortlichen Handlungsweise? Diese Fragen sind vom Gesetzgeber zu klären, bevor umfassende Normenkonstrukte erlassen werden. Denn übertriebene und hochkomplexe Gesetzesvorlagen verkommen letztlich zur symbolischen Gesetzgebung, wenn sie weder durchgesetzt noch beachtet werden. Statt steigendes Vertrauen erntet man Misstrauen: der Rechtsstaat wird untergraben.

- **Notwendige Anpassungen an internationales Recht mit Augenmass**: Die Notwendigkeit einer Revision des DSG ergibt sich daher aus Sicht der IHZ grösstenteils aufgrund der Rechtsentwicklung auf internationaler Ebene. Wettbewerbsnachteile aufgrund eines im internationalen Vergleich mangelhaften Datenschutzes sind zu verhindern. Hier muss der Gesetzgeber den vorhandenen Spielraum jedoch viel besser nutzen als im Entwurf geplant. Der Revisionsentwurf führt unbedarft Regelungen ein, ohne deren konkreten Auswirkungen zu kennen. Selbst der vorliegenden RFA gelingt es nicht, der Vorlage ein „Preisschild“ zu verpassen. Deshalb sind die im Vergleich zum EU-Raum überschiessenden Regulierungen dringend anzupassen. Ein unnötiger „swiss-finish“ ist unbedingt zu verhindern. Nur so garantiert man den Unternehmen ein Maximum an Flexibilität

und ein Minimum an zusätzlicher finanzieller Belastung. Als Beispiel für die überschiessenden Regulierungen sind die zahlreichen Informations- und Meldepflichten der Unternehmen zu erwähnen. Sie führen zu unverhältnismässigem Aufwand, generieren ihrerseits eine Informations- und Datenflut und wirken sich dadurch v.a. innovations- und wettbewerbshindernd aus. So behindert das geplante DSG die Ausschöpfung des vorhandenen Potentials der Digitalisierung und schmälert den Nutzen derselben unnötig. Der Gesetzgeber soll deshalb nachbessern und Innovation und Entwicklung im Interesse der Unternehmen und Konsumenten stärker fördern und nicht gesetzlich unterbinden.

- **Selbstregulierung fördern**: Die IHZ ist zudem überzeugt, dass neben der Ausnützung des erwähnten Spielraumes auch das etablierte System der Selbstregulierung weiterhin gefördert werden muss. Selbstregulierung mit starkem Praxisbezug ermöglicht, im Gegensatz zu abstrakten Gesetzesvorlagen, die Realisierung von realitätsnahen und sachgerechten Lösungen.

Fazit

Die IHZ anerkennt grundsätzlich das Bedürfnis, das DSG zu revidieren. Angesichts der technologischen Entwicklung gilt es den internationalen Entwicklungen Rechnung zu tragen. Dies besonders, um im EU-Raum den Status eines angemessenen Datenschutzes nicht zu riskieren. Der vorliegende Entwurf fällt jedoch durch übertriebene Bestimmungen auf („swiss-finish“), die bei den Unternehmen zu unnötigem administrativem Aufwand und Mehrausgaben führen, ohne den Datensubjekten substantielle Vorteile zu bringen. Das DSG würde in der vorliegenden Form für den Schweizer Wirtschaftsstandort im internationalen Vergleich zu Wettbewerbsnachteilen führen. Wir fordern den Gesetzgeber auf, innerhalb der internationalen Vorgaben den Spielraum besser auszunutzen, um dem Schweizer Wirtschaftsstandort ein Maximum an Flexibilität zu erhalten. In Bezug auf konkrete Anpassungen zu den einzelnen Rechtsnormen verweisen wir auf die Vernehmlassungsantwort der economiesuisse.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Industrie- und Handelskammer Zentralschweiz

Die Schweizer Journalist*innen I giornalisti svizzeri
impressum Les journalistes suisses

Au Département fédéral de Justice et police
Confédération suisse

Fribourg, le 4 avril 2017

Concerne : Procédure de consultation sur l'avant-projet de loi fédérale sur la protection des données – Prise de position d'impressum – Les journalistes suisses

Madame, Monsieur,

im**pres**sum – Les journalistes suisses, l'organisation professionnelle des journalistes la plus importante de Suisse, a l'avantage de prendre ainsi position dans le cadre de la procédure de consultation ouverte le 21 décembre 2016.

Nous avons pris connaissance de l'avant-projet de loi.

Nous saluons le maintien à l'article 22 AP-LPD de l'article 10 LPD consacré aux restrictions du droit d'accès applicable aux médias.

Cette disposition est très importante pour les médias et le travail journalistique et c'est donc très important de la maintenir matériellement comme elle se trouve dans la législation actuelle. Cette disposition sert la liberté de presse et de l'information.

Nous vous prions de croire, Madame, Monsieur, à l'assurance de nos salutations distinguées.

im**pressu**m – Les journalistes suisses

Dominique Diserens, Dr. iur., Secrétaire centrale

Zentralsekretariat Secrétariat central Segretariato centrale

Rue Fries 2, Case postale 1701 Fribourg
Tél. ++41+26 347 15 00 Fax ++41+26 347 15 09
www.impressum.ch info@impressum.ch

Amstutz Jonas BJ

Von: Flück, Caspar <Caspar.Flueck@insel.ch>
Gesendet: Dienstag, 28. März 2017 09:00
An: Amstutz Jonas BJ
Cc: Kiser, Rebekka; Flückiger, Jacqueline
Betreff: Vernehmlassung VDSG
Anlagen: Insel Gruppe AG_Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme.doc

Sehr geehrter Herr Amstutz

Beiliegend erhalten Sie die Vernehmlassungsantwort der Insel Gruppe AG zum Vorentwurf des revidierten Datenschutzgesetzes. Wir danken Ihnen für die uns gewährte Möglichkeit zur Stellungnahme und verbleiben

Mit freundlichen Grüssen

Caspar Flück, lic. iur., MPA
Stv. Leiter Recht & Compliance, Compliance Officer

Insel Gruppe AG, Inselspital
Recht & Compliance
Effingerstr. 77, 1.104
3010 Bern

Telefon: +41 (0)31 632 95 90
E-Mail: caspar.flueck@insel.ch
www.insel.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Insel Gruppe AG

Abkürzung der Firma / Organisation : Insel

Adresse : Freiburgstrasse 18, 3010 Bern

Kontaktperson : Rebekka Kiser, Datenschutzbeauftragte Insel Gruppe AG

Telefon : 031 632 38 73

E-Mail : rebekka.kiser@insel.ch

Datum : 28.03.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Insel	Betrieblicher Datenschutzbeauftragter Es wäre wünschenswert, wenn die Bestimmungen zum betrieblichen Datenschutzbeauftragten wieder Eingang in das revidierte Datenschutzgesetz finden würden (analog der bisherigen Regelung in Art. 11a DSG und Art. 12b VDSG). Wie bis anhin, sollte die Schaffung einer solchen Stelle mit dem Vorteil einhergehen, dass das Unternehmen von gewissen Pflichten (z.B. Informations- und Meldepflicht/en) entbunden wird. Damit würde man auch einen grossen Anreiz für die Unternehmen schaffen eine solche Stelle zu besetzen und der Beauftragte/EDÖB könnte erheblich entlastet werden.
Insel	Meldepflichten Es ist unklar, welchen Sinn und Zweck die im VE-DSG statuierten Meldepflichten an den EDÖB verfolgen. Die Art und Weise der Datenbearbeitung durch den EDÖB selber ist ebenfalls nicht hinreichend geregelt. Zudem zeichnet sich ein grosser administrativer Aufwand nicht nur durch die Datenbearbeiter, sondern in noch viel massiveren Ausmass für den EDÖB selber ab; wird dem nicht mit der Beschaffung von erheblich mehr Ressourcen entgegengewirkt, sind diese Bestimmungen von vornherein zum Scheitern verurteilt.
Insel	Verhältnis zur europäischen DSGVO Es ist nicht nachvollziehbar, aus welchen Gründen die Vorschriften der europäischen Datenschutzgrundverordnung teilweise massiv verschärft wurden, ohne dass ein erheblicher Mehrwert ersichtlich wäre.
Insel	Allgemeines Fazit zum VE-DSG Insgesamt zeigt der VE-DSG in seiner jetzigen Form, unserer Ansicht nach, erhebliche Schwächen und bedarf einer grundlegenden Überarbeitung. Insbesondere hinsichtlich der Praxistauglichkeit bestehen massgebliche Lücken und unausgereifte Neuregelungen. Wir regen deshalb an, unsere Rückmeldungen zu prüfen und die erforderlichen Anpassungen im Vorentwurf vorzunehmen. Die Ziele des Datenschutzes und dessen Akzeptanz sind nur durch eine praxisnahe Ausgestaltung der datenschutzrechtlichen Rechtsbestimmungen zu erreichen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Insel	VE-DSG	3			neuer Bst.: Definition von „private Person“: natürliche oder juristische Person des Privatrechts
Insel	VE-DSG	3		f.	Das „Profiling“ fällt nur unter die Bestimmungen des Datenschutzgesetzes, wenn Personendaten bearbeitet werden. Der Begriff „Daten“ sollte deshalb vorliegend gestrichen werden und es sollte einzig die Auswertung von Personendaten erwähnt werden. Damit werden auch (Personen)daten erfasst die zu Beginn noch keiner Person zugeordnet werden können, aber in Kombination mit anderen die Identifikation ermöglichen („bestimmbar“; vgl. auch Definition in Art. 4 Ziffer 4. EU-Datenschutzgrundverordnung (DSGVO)). Zudem sollte, wie auf europäischer Eben, einzig die automatisierte Bearbeitung den Begriff des „Profiling“ erfüllen. Die im Vorentwurf gewählte Umschreibung des „Profiling“, welche „jede Auswertung“ umfasst, weitet den Geltungsbereich massiv aus und erfasst bspw. auch das handschriftliche Ausfüllen des Mitarbeiter-Beurteilungsbogens oder das Erstellen eines ärztlichen Behandlungsplans. Auf eine solche Ausweitung ist zu verzichten und der Text wie folgt abzuändern „jede automatisierte Auswertung (…)“ Der Begriff „Profiling“ ist allgemein sehr auslegungsbedürftig und sollte mindestens in der Botschaft zum revidierten DSG in hohem Detaillierungsgrad umschrieben werden (vgl. nachfolgende Anmerkungen zum Erläuternden Bericht).
Insel	VE-DSG	3		h.	Die Bezeichnung „private Person“ führt zu Unklarheiten, wer oder welche Personen gemäss VE-DSG als „Verantwortlicher“ gelten. Empfehlung: „private Person“ sollte vorliegend durch „natürliche oder juristische Person des Privatrechts“ ersetzt werden (vgl. auch Art. 4 Ziffer 7. DSGVO). Alternativ kann bereits der Begriff „private Person in diesem Artikel definiert werden (vgl. Ausführung oben).
Insel	VE-DSG	3		i.	Der Begriff „Auftragsbearbeiter“ ist unserer Ansicht nach unklar definiert, so dass dies auch ein Mitarbeiter einer juristischen Person sein könnte. Aus der Definition des Begriffs sollte klar ersichtlich

					sein, dass der Auftragsbearbeiter nur eine unternehmensfremde Person oder Stelle sein kann (folglich ein Dritter).
Insel	VE-DSG	4	3		Beim Erfordernis, dass Personendaten zu einem „klar erkennbaren Zweck beschafft werden“, sollte das Wort „klar“ gestrichen werden. Dies weil damit grosse Unsicherheiten verbunden sind, welche Bedingungen erfüllt sein müssen, um von einem „klar“ erkennbaren Zweck sprechen zu können.
Insel	VE-DSG	4	4		Absatz ergänzen durch „Vorbehalten bleiben gesetzliche Aufbewahrungs- und Archivierungsvorschriften.“
Insel	VE-DSG	4	6		Welches die Anforderung an die „Ausdrücklichkeit der Einwilligung“ sind, sollte mindestens in den „Erläuterungen zu den einzelnen Artikeln“ bzw. in der Botschaft beschrieben werden.
Insel	VE-DSG	5	4		Der Absatz sollte zur Klarheit ergänzt werden durch: „Bringt der Beauftragte innert der vorgegebenen Frist keine Einwände vor oder verzichtet auf solche, ist der Verantwortliche berechtigt die Daten ins Ausland bekannt zu geben.“
Insel	VE-DSG	5	5		Um Vorhaben nicht unnötig zu verzögern und dadurch Unternehmen in ihrer Wirtschaftsfreiheit einzuschränken, sollte die Frist für die Rückmeldung des Beauftragten von 6 auf 3 Monate gekürzt werden. Es ist klarzustellen, dass diese Frist eine Verwirkungsfrist darstellt und vom EDÖB nicht verlängert werden kann. Zudem sollte der Absatz der Klarheit halber wie folgt ergänzt werden: „Bestehen seitens Beauftragten keine Einwände oder ist die Frist ohne Vorbringen von solchen abgelaufen, so ist der Verantwortliche berechtigt Daten ins Ausland bekannt zu geben.“
Insel	VE-DSG	5	6		Die Bestimmung sollte ersatzlos gestrichen werden. Nachdem die standardisierten Garantien bereits dem Beauftragten zur Genehmigung vorgelegt werden müssen (Art. 5 Abs. 3 Bst. c VE-DSG), erscheint eine erneute Information über den Gebrauch der Garantien unverhältnismässig. Dass sowohl Verantwortlicher als auch Auftragsbearbeiter zur Information an den Beauftragten verpflichtet werden, führt zudem zu Unklarheiten betreffend der Zuständigkeiten.
Insel	VE-DSG	6	1	c Ziff. 2	Es wird empfohlen das „vor Gericht und Verwaltungsbehörde“ gestrichen wird, da mit dieser Umschreibung nicht sichergestellt ist, dass alle Behörden und Stellen erfasst werden, vor denen

					Rechtsansprüche durchgesetzt oder abgewehrt werden sollen. Zudem könnten in der Auslegung der Begrifflichkeiten „Gericht und Verwaltungsbehörde“ im Ausland Unklarheiten entstehen, mit einer Streichung kann dem entgegengewirkt werden.
Insel	VE-DSG	6	2		Die Meldepflicht sollte ersatzlos gestrichen werden. Zum einen werden mit der Meldepflicht ggf. höher zu gewichtende Interessen des Unternehmens verletzt (da die zu liefernden Informationen dem Berufsgeheimnis oder dem Geschäftsgeheimnis unterstehen). Dies insbesondere vor dem Hintergrund, dass alle an den EDÖB gelieferten Informationen grundsätzlich gemäss Öffentlichkeitsgesetz einsehbar sind. Zum anderen ist nicht definiert, was der Beauftragte mit diesen Meldungen macht (dies im Gegensatz zu den Zusammenarbeitspflichten gemäss Art. 5 Abs. 4 und 5 VE-DSG) und zudem ist wiederum unklar, wer für die Meldung verantwortlich ist (der Auftragsbearbeiter oder der Verantwortliche). Vergleich zu dem auch den Hinweis in den „Allgemeinen Bemerkungen“ zur Meldepflicht.
Insel	VE-DSG	7	1	b	Vorliegend sollte das Wort „ausdrücklich“ eingefügt werden (d.h. „(…) die Übertragung ausdrücklich verbietet“). Insbesondere bei der Bearbeitung von Patienteninformationen, welche dem Berufsgeheimnis, unterstehen, werden in der Rechtslehre und Gerichtspraxis betreffend der Zulässigkeit der Auftragsdatenbearbeitung unterschiedliche Standpunkte eingenommen. Mit der vorgeschlagenen Ergänzung könnte für mehr Klarheit gesorgt werden. Es wäre zudem sehr begrüssenswert, wenn die Botschaft die Übertragung der Bearbeitung von Daten, welche unter dem Schutz einer gesetzlichen Geheimhaltungspflicht stehen, an einen Auftragsbearbeiter detailliert ausführt.
Insel	VE-DSG	7	2		Der Bundesrat sollte aus rechtsstaatlicher Sicht einzig befugt werden die in Art. 7 VE-DSG festgehaltenen Grundsätze zu konkretisieren, zumindest das Wort „weitere“ (Pflichten) sollte deshalb gestrichen werden.
Insel	VE-DSG	8			Grundsätzlich sind die Empfehlungen der guten Praxis zu begrüssen. Mit dieser Bestimmung erhält der EDÖB aber das eigenständige Recht, zumindest „teil-verbindliche“ Regeln zu erlassen und dies ohne Möglichkeit einer gerichtlichen oder überinstanzlichen Überprüfung. Es wäre zu prüfen, ob nicht ein unabhängiges Gremium die „Empfehlungen der gute Praxis“ verabschieden sollte oder ob die seitens

					EDÖB erarbeiteten Empfehlungen mindestens zwingend im Rahmen einer breit angelegten Vernehmlassung kommentiert und geprüft werden sollten. In der vorgeschlagenen Formulierung „(…) zieht dazu die interessierten Kreise bei (…)“ obliegt dem EDÖB die Entscheidung, bei wem die Meinungsbildung erfolgen soll. Statt der Formulierung betreffend „Beizug interessierter Kreise“, sollte deshalb im Gesetz (zusätzlich) eine zwingende Vernehmlassung oder Überprüfung durch eine übergeordnete Instanz verankert werden.
Insel	VE-DSG	12			Die Bestimmung ist ersatzlos zu streichen oder mindestens zu ergänzen (vergleiche nachfolgender detaillierter Vorschlag zu Art. 12 neu: c VE-DSG). Die Bestimmungen unter Art. 12 VE-DSG zum Thema „Daten einer verstorbenen Person“ erzeugt wenig Mehrwert, da bereits unter der heutigen Gesetzgebung die Möglichkeit besteht über verstorbene Personen Auskunft zu erhalten (auch wenn die diesbezügliche Bestimmung auf Verordnungsebene wegfallen sollten (Art. 1 Abs. 7 VDSG)). Die neu vorgesehen Bestimmung widerspricht der vorherrschenden Meinung hinsichtlich Andenkensschutz der verstorbenen Person, bringt sehr viele Unsicherheiten und gefährdet gesetzliche Geheimhaltungspflichten. Entgegen dem sonst klar erkennbaren Streben im VE-DSG, den Schutz der Personen bei der Bearbeitung ihrer Daten zu erhöhen, wird in dieser Vorschrift die verstorbene Person von jedem Schutz befreit und eine Datenbekanntgabe nicht nur ohne weiteres ermöglicht, sondern auch geheimnisbeschwerte Personen wie insb. Ärzte zur Auskunft verpflichtet. Dies ist weder nachvollziehbar noch notwendig.
Insel	VE-DSG	12	1	neu: c	Nachfolgend auf Bst. a. und b. sollte Bst. c. ergänzt werden mit folgendem Wortlaut: „c. keine gesetzlichen Geheimhaltungspflichten entgegenstehen“. Insbesondere vor dem Hintergrund, dass das ärztliche Berufsgeheimnis auch nach dem Tod eines Patienten noch Geltung hat, kann es nicht sein, dass dieser fundamental wichtige Rechtsgrundsatz durch vorliegende Gesetzesbestimmung ausgehebelt wird. Zumal ein schutzwürdiges Interesse bei nahen Verwandten, Ehepartner, eingetragenen Partner oder faktischer Lebenspartner bereits vermutet wird (Art. 12 Abs. 2 VE-DSG). Gerade die letzte Bezeichnung ist angesichts des Umstandes, dass Amts- und Berufsgeheimnisse ausser Kraft gesetzt werden, viel zu unklar und müsste gegebenenfalls durch die Definition aus dem Erwachsenenschutz ersetzt werden: „(…) oder mit ihr einen gemeinsamen Haushalt

					geführt hat und ihr regelmässig und persönlich Beistand geleistet hat." Eine Auskunft an Angehörige ist durch Einfügen der eingangs vorgeschlagenen Ergänzung nicht verwehrt, sondern das Behandlungsteam hat die Möglichkeit einzelfallgerecht zu entscheiden und sich je nach Fall durch die Aufsichtsbehörde/ den Kantonsarzt vom Berufsgeheimnis entbinden zu lassen. D.h. die gewünschte Auskunft wird bei Vorliegen eines begründeten Interesses in aller Regel erteilt, jedoch ohne Auferlegung einer Pflicht, welche das ärztliche Berufsgeheimnis und dessen Zielrichtung (nämlich das Vertrauensverhältnis zum Patienten zu schützen) erheblich belasten würde.
Insel	VE-DSG	12	3		Ersatzlos streichen, da eine grundlegende Schutzvorschrift ohne erkennbaren Grund ausgehebelt wird. Sollte die Bestimmung nicht gestrichen werden, zumindest den Satz ergänzen: „(…) davon ausgenommen ist das ärztliche Berufsgeheimnis bzw. das Berufsgeheimnis der Gesundheitsfachpersonen" (gemäss kantonaler Gesetzgebung).
Insel	VE-DSG	12	4	neu: c.	Nachfolgend auf Bst. a. und b. sollte Bst. c ergänzt werden mit folgendem Wortlaut: „c. der Löschung oder Vernichtung stehen gesetzliche Aufbewahrungs- oder Archivierungspflichten entgegen."
Insel	VE-DSG	13			Die Bestimmung ist unserer Ansicht nach in verschiedenster Hinsicht unpräzise und es sollten zumindest klare Mindestanforderungen definiert werden (evt. auch im Rahmen der geplanten „Empfehlungen der guten Praxis"). So ist nicht ganz klar, über was und wie umfassend informiert werden muss, sowie in welcher Form. Auch sollte festgelegt werden, dass eine Informationspflicht einzig im Zeitpunkt der Beschaffung von Personendaten besteht. Dies sollte spätestens in der Verordnung konkretisiert werden oder bereits im Gesetz (bspw. in Anlehnung an die Inhalten gemäss Art. 13 und 14 DSGVO), dies insbesondere vor dem Hintergrund, dass die Verletzung der Bestimmung strafrechtlich massiv sanktioniert werden soll (Art. 50 Abs. 1 VE-DSG).
Insel	VE-DSG	13	4		Die Informationspflicht betreffend Auftragsbearbeiter sollte ersatzlos gestrichen werden. Zum einen müsste der Verantwortliche dadurch einen Teil seiner Geschäftsbeziehungen offenlegen, zum anderen ist der Mehrwert dieser Information für die betroffene Person sehr beschränkt. Wenn überhaupt, sollte einzig vorgesehen werden, dass die betroffene Person im Rahmen des individuellen Auskunftsrecht diese Information verlangen kann (Art. 14 VE-DSG).

Insel	VE-DSG	14	4	a	Die Anforderung „(…) und er die Personendaten nicht an Dritte bekannt gibt“, sollte unserer Ansicht nach gestrichen werden, da letztendlich betreffend Verzicht, Aufschub oder Einschränkung der Information nur entscheidend sein darf, ob das Interesse des Verantwortlichen gegenüber dem Interessen der betroffenen Person überwiegt (unabhängig davon ob die Daten an Dritte bekannt gegeben werden oder nicht).
Insel	VE-DSG	16	1		Im Spitalumfeld werden vorderhand Patientendaten, also besonders schützenswerte Personendaten, bearbeitet. Damit wird die Anforderung des „erhöhten“ Risiko in der Regel in den meisten Fällen der Datenbearbeitung erfüllt sein, mit der Folge das unzählige Datenschutz-Folgeabschätzungen durchgeführt und dem Beauftragten vorgelegt werden müssten. Dies würde zur Folge haben, dass viele notwendige Projekte massiv verzögert und seitens der Unternehmen/Spitäler einzig für diese Tätigkeit erhebliche zusätzliche Ressourcen bereitgestellt werden müssten. Artikel 35 DSGVO beschränkt die Pflicht auf Datenbearbeitungen mit „hohen“ Risiken und führt zudem detaillierter aus, in welchen Fällen von einem hohen Risiko auszugehen ist. Das revidierte Datenschutzgesetz sollte nicht einschneidendere Bestimmungen vorsehen, ohne dass ein Mehrwert erkennbar wäre, und entweder im Gesetz selber oder in der Verordnung Konkretisierungen vornehmen. In diesem Zusammenhang wäre auch zu klären, ob für bestehende Datenbearbeitungen eine solche Folgenabschätzung vorgenommen werden muss und die Folgenabschätzung erneuert bzw. wiederholt werden muss, wenn sich die Form oder die Risiken der Datenbearbeitung ändern.
Insel	VE-DSG	16	4		Der Beauftragte/EDÖB sollte nur konsultiert werden müssen, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm ergriffenen Schutzmassnahmen ein hohes Risiko für eine Verletzung der Persönlichkeit der betroffenen Personen verbleibt (analog der Bestimmung in der EU; Art. 36 DSGVO). Zudem sollte die Frist zur Geltendmachung von Einwänden auf maximal 8 Wochen verkürzt werden (ebenfalls analog den Bestimmungen der DSGVO). Werden innert der vorgegebenen Frist seitens Beauftragten keine Einwände vorgebracht, sollten die im Rahmen der Folgenabschätzung vorgesehenen Massnahmen Geltung haben.
Insel	VE-DSG	17	1		In einem Spitalbetrieb unserer Grösse wird täglich eine grosse Menge an Personendaten durch unzählige Mitarbeitende bearbeitet. Unbefugte Datenbearbeitungen oder Datenverluste können daher in der Regel

					nur festgestellt werden, wenn konkrete Hinweise auf eine Datenschutzverletzung vorliegen. Vor diesem Hintergrund ist unklar, wen die in Art. 17 VE-DSG statuierte Meldepflicht konkret trifft. Ist diejenige Person zur Meldung verpflichtet, welche die unbefugte Datenbearbeitung vornimmt oder den Verlust der Daten verursacht? Oder ist es diejenige Person, welche die Datenschutzverletzungen feststellt? Oder obliegt die Meldepflicht immer dem Datenschutzbeauftragten eines Unternehmens (sofern dieser die Verletzung überhaupt feststellt)? Da die Verletzung der Meldepflicht nach Art. 50 Abs. 2 Bst. e (*recte* d) strafbar ist, regen wir dringend an, das Gesetz diesbezüglich zu präzisieren, auch betreffend Inhalt und Umfang der Meldepflicht. Im Weiteren regen wir an, dass der Umfang der meldepflichtigen Vorfälle auf solche beschränkt wird, in denen eine Verletzung des Schutzes personenbezogener Daten festgestellt wird (bspw. das Hacken in ein Computersystem). Denn mit vorliegender Bestimmung geht man in unverhältnismässigerweise über die Bestimmungen der DSGVO (Art. 33) hinaus und erfasst jede Datenbearbeitung, die gegen das DSG verstösst, auch beispielsweise die zweckfremde oder unverhältnismässige Nutzung von Daten. Sowohl die betroffenen Verantwortlichen/Unternehmen als auch der EDÖB wären mit solch einer Regelung und der damit einhergehenden Bearbeitung von Meldungen überlastet, was eine sach- und zeitgerechte Reaktion auf Verletzungen weitestgehend verunmöglicht und damit im Widerspruch zur Zielrichtung der Bestimmung steht (nämlich auf Gefährdungen und Verletzungen des Persönlichkeitsrechts adäquat zu reagieren). Zudem sollte die Meldepflicht auch in zeitlicher Sicht angepasst werden: statt „unverzüglich“, sollte die Meldung „ohne unnötigen Verzug“ erfolgen. Dies ist sinnvoll, da der Verantwortliche dadurch ausreichend Zeit hat die Hintergründe der Verletzung zu erforschen. Im Gegensatz zu Art. 12 Abs. 3 VE-DSG kann man sich vorliegend auf das Berufsgeheimnis berufen. Wir gehen daher davon aus, dass die unbefugte Bearbeitung oder der Verlust von Patientendaten dem Beauftragten nicht gemeldet werden müssen, da diese Daten durch das Berufsgeheimnis geschützt sind. Wir regen an, zumindest in den Erläuterungen auf diesen Vorbehalt zu Gunsten des Berufsgeheimnisses hinzuweisen.
Insel	VE-DSG	19		a	Im Erläuternden Bericht zum VE-DSG wird ausgeführt, dass Art. 19 Bst. a. VE-DSG die bisherige Pflicht Privater ersetzen soll, Datensammlungen beim Beauftragten zu registrieren (S. 65). Dies kommt unserer Ansicht nach viel zu wenig aus der Bestimmung heraus, denn sie spricht nicht von Datensammlungen

					und deren Bearbeitung, sondern im Allgemeinen von Datenbearbeitungen, was an sich uferlos ist. Auf europäischer Ebene sind zwar auch solche Dokumentationspflichten vorgesehen, doch im Gegensatz zum Vorentwurf in stark begrenztem Masse (vgl. Art. 30 DSGVO). Zwar wird im Erläuternden Bericht darauf hingewiesen, dass in der Verordnung konkretisiert werden soll, welche Angaben dokumentiert werden sollen, doch sollte auch in Bezug auf dem Umfang der Datenbearbeitung Ausführungen gemacht werden. Sollte die Verordnung zum revidierten DSG nicht gleichzeitig mit dem DSG Inkrafttreten, wäre zudem wünschenswert, wenn die Konkretisierung auf Gesetzesebene erfolgt, dies insbesondere vor dem Hintergrund, dass vorgesehen ist Verstösse gegen Dokumentationspflichten massiv zu sanktionieren (vgl. Art. 51 Bst. f VE-DSG). Im Grundsatz ist es aber zu begrüssen, dass die Registrierungspflicht von Datensammlungen beim Beauftragten zukünftig wegfallen soll.
Insel	VE-DSG	19		b	Die Bestimmung sollte ersatzlos gestrichen werden. Die Rechte der betroffenen Person betreffend Mitteilung an Empfänger von Personendaten sind ausreichend in Art. 25 Abs. 3 VE-DSG geregelt. Im Spitalumfeld und insbesondere in einem Grossbetrieb wie der Insel Gruppe AG wird täglich unzählige Male nach aussen hin kommuniziert, sei dies gegenüber zuweisenden Ärzten, weiterbehandelnden Ärzten, Patienten, Versicherungen oder Behörden. Nicht jede dieser Kommunikationsvorgänge kann und wird nachvollziehbar dokumentiert. Zu ermitteln, wer alles die Empfänger von Personendaten sind, ist vor diesem Hintergrund annähernd unmöglich. Im weiteren ist der Umfang an Vorfällen, in denen Empfänger informiert werden müssen, unserer Ansicht nach viel zu umfassend und widerspricht der Bestimmung von Art.17 Abs. 2 VE-DSG, nach welcher die betroffene Person über Verletzungen des Datenschutzes nur falls erforderlich informiert wird. Sollte die Bestimmung nicht ersatzlos gestrichen werden, sollte sie zumindest dahingehend abgeschwächt werden, dass nur die Berichtigung, Löschung und Vernichtung von widerrechtlich bearbeiteten Daten von der Bestimmung erfasst werden (Abgrenzung von Löschung/Vernichtung von Daten nach Ablauf der Aufbewahrungspflicht). Die Information der Empfänger sollte zudem nur auf Wunsch/Antrag der betroffenen Person erfolgen müssen und nur gegenüber einem dem Verantwortlichen bekannten Empfänger oder von der betroffenen Person bezeichneten Empfängern. Im Weiteren sollte die betroffene Person diesen Anspruch nur geltend machen können, wenn sie/er ein schützenswertes Interesse hat. Eine Informationspflicht sollte zudem nur bestehen wenn die Löschung, Vernichtung oder

					Berichtigung entweder auf Veranlassung des Verantwortlichen vorgenommen worden ist, die betroffene Person dies gewünscht hat und seitens Verantwortlichen dem Wunsch entsprochen wurde oder aufgrund einer Klage zum Schutz der Persönlichkeit nach Art. 25 VE-DSG/28 f. ZGB zu erfolgen ist.
Insel	VE-DSG	44	3		Diese Bestimmung sollte ersatzlos gestrichen werden. Der Grundsatz, dass eine Beschwerde aufschiebende Wirkung hat, sollte bestehen bleiben. Wird die aufschiebende Wirkung per se entzogen, kann dies unter Umständen zu hohem Schaden führen und die betroffene Partei wird unter dem Druck der vorsorglichen Massnahmen ggf. Handlung oder Unterlassungen vornehmen, zu denen sie rechtlich gar nicht verpflichtet wäre und die sich im Nachhinein als falsch herausstellen könnten. Dieses Risiko besteht insbesondere vor dem Hintergrund, dass Art. 42 VE-DSG, welche die Grundlage für den Erlass von vorsorglichen Massnahmen bildet, sehr offen formuliert ist. Damit vorsorgliche Massnahmen nicht als eigentliches Druckmittel missbraucht werden können, sollte die aufschiebende Wirkung weiterhin gegeben sein. Der Beauftragte oder die zuständige Beschwerdeinstanz hat jederzeit die Möglichkeit den Entzug der aufschiebenden Wirkung zu beantragen bzw. die aufschiebende Wirkung zu entziehen. Der Beauftragte erhält mit dem Bestimmungen des VE-DSG schon sehr viele zusätzliche Eingriffsrechte und Kompetenzen, diese Rechte sollten nicht uferlos ausgebaut werden.
Insel	VE-DSG	50			Wir empfehlen die Bestimmung ersatzlos zu streichen oder umfassend zu überarbeiten (dazu nachfolgend). Eine Busse von bis zu CHF 500‘000 ist unserer Ansicht nach viel zu hoch, insbesondere vor dem Hintergrund, dass das Bussgeld vorderhand von der/den für die Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten verantwortliche/n natürlichen Person/en bezahlt werden muss/müssen. Viele der im VE-DSG festgehaltenen Pflichten werden in einem Unternehmen zukünftig einer gewissen Person oder einem gewissen Personenkreis zugeteilt werden (z.B. dem Datenschutzbeauftragten, dem IT-Sicherheitsbeauftragten), mit der stets drohenden Busse wird es schwer sein diese Rolle wahrzunehmen oder überhaupt Personen zu finden, welche bereit sind die damit einhergehenden Risiken zu tragen. Wurde die Verletzung von Auskunfts-, Melde- und Mitwirkungspflichten von Mitarbeitenden in einem Unternehmen begangen, sollte deshalb einzig das Unternehmen direkt gebüsst werden (vgl. auch Art. 83 DSGVO). Zudem sollten bereits auf gesetzlicher Ebene Kriterien definiert werden, nach welchen die Höhe

					der Busse festgelegt wird (vgl. Art. 83 DSGVO).
Insel	VE-DSG	50	1		Es ist vorliegend nicht klar, wer als antragsberechtigte Person gelten soll, da nur Personen antragsberechtigt sein können die durch eine Unterlassung der Auskunfts-, Melde- oder Mitwirkungspflicht verletzt sind. Sollte die Bestimmung in dieser Form verbleiben, sollte spätestens in der Botschaft detailliert ausgeführt werden, wer als antragsberechtigt gilt.
Insel	VE-DSG	50	2	e (*recte*: d)	Wir beantragen, dass Bst. e (*recte*: d) ersatzlos gestrichen wird. Diese Bestimmung stellt die Verletzung der Meldepflicht nach Art. 17 Abs. 1 VE-DSG unter Strafe. Wir erachten dies insbesondere dann als problematisch, wenn die zu meldende unbefugte Datenbearbeitung eine Verletzung der Sorgfaltspflicht gemäss Art. 51 VE-DSG darstellt und damit selber mit Busse bestraft wird. Die meldende Person steht vor dem Dilemma, sich aufgrund des gesetzlich stipulierten Meldungszwangs selber zu einer unter Strafe gestellten Datenschutzverletzung bekennen zu müssen. Dadurch wird der strafrechtliche Grundsatz „nemo tenetur se ipsum accusare“ verletzt. Niemand kann zu einem selbstbelastenden Verhalten gezwungen werden. Die Selbstbelastungsfreiheit ist heute als allgemeiner Grundsatz des Strafprozessrechts anerkannt und geniesst darüber hinaus in Rechtsprechung und Lehre verfassungsrechtlichen Rang. Vor diesem Hintergrund ist die Rechtmässigkeit von Art. 50 Abs. 2 Bst. e (*recte*: d) höchst fraglich.
Insel	VE-DSG	50	3	a	Empfohlenermassen ersatzlos zu streichen, da ebenfalls die Streichung von Art. 19 Bst. b VE-DSG beantragt wird.
Insel	VE-DSG	50	4		Die vorliegende Bestimmung sollte ersatzlos gestrichen werden. Die Bestrafung der fahrlässigen Tatbegehung führt zu einer massiv erhöhten Kriminalisierung von betroffenen Mitarbeitenden und Unternehmen, jedoch kaum zu einer Verbesserung des Datenschutzes (bisher ist beispielsweise die fahrlässige Verletzung des Berufsgeheimnisses nicht strafbar, dieser Status quo sollte beibehalten werden).
Insel	VE-DSG	51			Wir beantragen auch hier die ersatzlose Streichung oder eine Anpassung analog unserem Vorschlag zu Art. 50 VE-DSG.

					Es sei vorliegend auf zudem unsere Ausführungen zu Art. 5, 6, 7, 11, 16 und 19 VE-DSG verwiesen, wo wir insbesondere empfohlen haben, dass die Sorgfaltspflichten detaillierter umschrieben und eingegrenzt werden.
Insel	VE-DSG	51	1	a	Ist empfohlenermassen ersatzlos zu streichen, da ebenfalls die Streichung von Art.6 Abs. 2 VE-DSG beantragt wird.
Insel	VE-DSG	53			Werden die Strafbestimmungen von Art. 50 und 51 VE-DSG dahingehend angepasst, dass bei der Verletzung von Auskunfts-, Melde- und Mitwirkungspflichten sowie einer Verletzung von Sorgfaltspflichten einzig das Unternehmen mit Busse bestraft wird, kann diese Bestimmung ersatzlos gestrichen werden (vgl. obige Ausführungen zu Art. 50 und 51 VE-DSG).
Insel	VE-DSG	52/53			Artikel 52 VE-DSG sollte unserer Ansicht nach als Art. 53 geführt werden und Art. 53 VE-DSG als Art. 52. Dies da Art. 53 VE-DSG gemäss Erläuterndem Bericht (S. 86) einzig auf Art. 50 und Art. 51 VE-DSG Anwendung findet, bei Verletzungen der beruflichen Schweigepflicht nach zurzeit Art. 52 VE-DSG soll hingegen alleine Art. 102 StGB zur Anwendung kommen.
Insel	VE-DSG	59			Es ist nicht ersichtlich, weshalb die Übergangsfrist von zwei Jahren nur für bestimmte Pflichten des Verantwortlichen gelten sollen, dadurch fehlen wichtige Übergangsregelungen z.B. für die Meldung von Datenschutzverstössen oder die neuen Auskunfts- und Informationspflichten. Die neu statuierten Pflichten müssen in einem Grossbetrieb wie der Insel Gruppe AG zuerst umgesetzt und verantworlichen Personen zugewiesen werden, dies ist nicht von einem auf den anderen Tag möglich und bedarf einer ausreichenden Übergangsfrist. Es sollte deshalb für die Umsetzung des revidierten DSG eine generelle Umsetzungsfrist von zwei Jahren vorgesehen werden.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Insel	3 Bst. f.	Es wäre wünschenswert, wenn sich die zukünftige Botschaft zur Revision des DSG detaillierter mit dem Begriff „Profiling“ auseinandersetzt und auch mit der verlangten ausdrücklichen Zustimmung. Dies im Besonderen vor dem Hintergrund, dass die Aufzählung der betroffenen Bereiche, in denen von einem „Profiling“ gesprochen werden kann, in der derzeit vorgesehenen Gesetzesbestimmung nicht abschliessend ist und auch die Definition gemäss DSGVO erweitert.
Insel	3 Abs. 6	In der zukünftig folgenden Botschaft zur Revision des DSG sollte das Thema „Einwilligung“ und insbesondere die Anforderungen an die „Ausdrücklichkeit“ umfassender dargelegt werden,
Insel	5 Abs. 4, 5	Sollte die Bestimmung gemäss unserem Vorschlag angepasst werden, sollte in der zukünftigen Botschaft zur Revision des DSG festgehalten werden, dass es sich vorliegend nicht um Ordnungsfristen, sondern um nicht verlängerbare Verwirkungsfristen handelt.
Insel	7 Abs. 1	Es wäre sehr zu begrüssen, wenn die „Erläuterungen zu den einzelnen Artikel“ oder spätestens die Botschaft die Zulässigkeit der Übertragung der Datenbearbeitung - welche unter dem Schutz einer gesetzlichen Geheimhaltungspflicht stehen - an einen Auftragsbearbeiter detailliert umschreibt
Insel	17 Abs. 1	Im Gegensatz zu Art. 12 Abs. 3 VE-DSG kann man sich vorliegend auf das Berufsgeheimnis berufen. Wir gehen daher davon aus, dass die unbefugte Bearbeitung oder der Verlust von Patientendaten dem Beauftragten nicht gemeldet werden müssen, da diese Daten durch das Berufsgeheimnis geschützt sind. Wir regen an, zumindest in den Erläuterungen oder spätestens in der Botschaft zum Gesetz auf diesen Vorbehalt zu Gunsten des Berufsgeheimnisses hinzuweisen.
Insel	50 Abs. 1	Es ist in vorliegender Gesetzesbestimmung nicht klar, wer als antragsberechtigte Person gelten soll, da nur Personen antragsberechtigt sein können die durch eine Unterlassung der Auskunfts-, Melde- oder Mitwirkungspflicht verletzt sind. Sollte die Bestimmung in dieser Form verbleiben, sollte spätestens im Erläuternden Bericht und in der Botschaft detailliert ausgeführt werden, wer als antragsberechtigt gilt.

interpharma:ph

Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Jonas Amstutz
Bundesrain 20
3003 Bern

Basel, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Damen und Herren

Wir nehmen im Folgenden im Rahmen der Vernehmlassung zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz Stellung.

Interpharma ist der Verband der forschenden pharmazeutischen Firmen in der Schweiz. Wir äussern uns lediglich zu zwei Aspekten des Vorentwurfs. Im Übrigen verweisen wir auf die umfassende Stellungnahme von economiesuisse und scienceindustries.

Vorbemerkung

Ein angemessenes und wirksames Datenschutzgesetz ist für die Wirtschaft ein Erfordernis. Dieses muss Raum für die wirtschaftliche Entwicklung lassen sowie der Rechts- und Investitionssicherheit dienen. Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und der Nutzung des damit verbundenen wirtschaftlichen Potentials. Zu weit gehende und nicht praktikable Bestimmungen können sich demgegenüber im Wirtschaftsalltag hemmend auswirken. Sie können der Wettbewerbsfähigkeit von Unternehmen schaden. Zu weitgehende Bestimmungen, welche den Individuen ihre Handlungsfähigkeit absprechen, führen zudem zu einer Bevormundung der Bürger.

Für die Akteure der forschenden Pharmaindustrie ist von Bedeutung, dass der Zugang zum und der Verkehr mit den Ländern der EU auch aus Sicht des Datenschutzes hindernislos gewährleistet ist. Diesbezüglich muss das Ziel der Totalrevision sein, dass die Angemessenheitserklärung durch die Kommission der Europäischen Union (EU) behalten werden kann. Darüber hinaus hat sich das Schweizer Datenschutzrecht auch an der Konvention 108 des Europarates zu orientieren, welche für die Schweiz verbindlich gilt.

Interpharma, Petersgraben 35, Postfach, CH-4009 Basel, **Telefon +41 (0)61 264 34 00**, Telefax +41 (0)61 264 34 01
info@interpharma.ch, www.interpharma.ch, Verband der forschenden pharmazeutischen Firmen der Schweiz

Spezifische Anliegen der forschenden Pharmaindustrie

- Das Humanforschungsgesetz und dessen Verordnungen gehen als lex specialis dem „Querschnitt"-Gesetz DSG vor.
- Anpassung der Begriffe genetische, biometrische Daten und Profiling

Grundsatz der lex specialis

Der erläuternde Bericht zur DSG-Revision hält auf Seite 39 fest, dass aufgrund der lex specialis Regel grundsätzlich die bereichsspezifischen Datenschutznormen gelten. Interpharma begrüsst die Betonung dieses Grundsatzes, der dadurch in der Praxis den Vorrang des Humanforschungsgesetzes und aller entsprechenden Verordnungen zum Humanforschungsgesetz vor dem Datenschutzgesetz bewirkt.

Auf Seite 70 des erläuternden Berichts wird ausgeführt, dass die Bestimmung von Art. 24 Abs. 2 lit. e Ziff. 1 VE DSG (Rechtfertigungsgrund der Forschung, Planung und Statistik) inskünftig verschärft ausgelegt und deshalb nur noch erschwert angerufen werden kann, dies insbesondere auch im Kontext der Datenaufbewahrung (Art. 4 Abs. 4 VE DSG).

In Anbetracht des grundsätzlichen Vorrangs des Humanforschungsgesetzes sind die Aussagen zur Bestimmung von Art. 24 Abs. 2 lit. e Ziff. 1 VE DSG zu relativieren. Sie können für den Bereich der Humanforschung nicht gelten.

Interpharma fordert eine Klarstellung in der Botschaft zur Totalrevision des Datenschutzgesetzes, dass a) der Grundsatz der lex specialis gilt, b) das Humanforschungsgesetzes, das Vorrang vor dem DSG hat, explizit genannt wird und c) der Vorrang der lex specialis selbstredend für sämtliche mit der Spezialgesetzgebung in Zusammenhang stehenden Verordnungen gilt und dies ebenfalls explizit erwähnt wird. Damit wird für die Akteure in der Humanforschung und für den EDÖB sowie die Gerichte die notwendige Klarheit geschaffen.

Begriffe

<u>Genetische und biometrische Daten</u>

Bei der Definition der beiden Begriffe ist darauf abzustellen, ob sie zum Zweck der Identifizierung erhoben und bearbeitet werden. Die Eignung der genetischen und biometrischen Daten zur Identifizierung einer Person soll für die Definition der beiden Begriffe dagegen nicht im Vordergrund stehen. Es muss beispielsweise möglich sein, durch die Untersuchung von genetischen Daten Mechanismen zu erforschen. Die Identität der DNA-Spender ist dabei nicht von Interesse und deren Identifizierung wird in der Praxis weder bezweckt noch faktisch angestrebt oder tatsächlich herbeigeführt.

Profiling

Das Profiling-Konzept des Vernehmlassungs-Entwurfs ist einschränkender als das internationale Regelwerk und geht über die Bestimmungen der europäischen Datenschutz-Grundverordnung und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der europäischen Grundverordnung noch in der Konvention vorgesehen.

Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren, und eine darauf gestützte Entscheidung für die betroffene Person rechtliche Folgen oder erhebliche Auswirkungen hat.

Das Erfordernis der vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling erscheint als übermässig streng. Profiling soll erst schutzrelevant werden, wenn es um die Verwendung des Profils im Rahmen einer automatisierten Entscheidung mit Rechtsfolge geht und nicht bereits bei dessen Erstellung.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und ersuchen Sie um Berücksichtigung unserer Erwägungen. Für Rückfragen oder ergänzende Erläuterungen, sehr geehrte Damen und Herren, stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

INTERPHARMA

Dr. Heiner Sandmeier
Generalsekretär a.i.

Bruno Henggi
Leiter Public Affairs

Amstutz Jonas BJ

Von: Ursula Widmer <ursula.widmer@widmer.ch>
Gesendet: Montag, 3. April 2017 12:13
An: Amstutz Jonas BJ
Betreff: Stellungnahme ISSS zum Datenschutzgesetz
Anlagen: Stellungnahme_ISSS_2017.03.28_final.doc
Signiert von: ursula.widmer@widmer.ch

Sehr geehrte Damen und Herren

Als angehängte Datei erhalten Sie im Namen von ISSS die Stellungnahme zum neuen Datenschutzgesetz.

Die Information Security Society Switzerland (ISSS; www.isss.ch) ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander. ISSS ist offizieller ICT Security Fachpartner von SwissICT.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und dem Informationsschutz der Schweiz leisten können und danken Ihnen für die Berücksichtigung unserer Anträge.

Freundliche Grüsse

Ursula Widmer
Past President ISSS / Leitung ISSS Task Force Revision Datenschutz

Dr. Widmer & Partner, Rechtsanwälte
Schosshaldenstrasse 32
CH-3000 Bern 31
Tel. +41 31 351 66 33
Fax +41 31 351 66 50
ursula.widmer@widmer.ch
www.widmer.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation	: **Information Security Society Switzerland**
Abkürzung der Firma / Organisation	: **ISSS**
Adresse	: Bollwerk 21, 3011 Bern
Kontaktperson	: Dr. Ursula Widmer, Rechtsanwältin, Past President ISSS / Leitung ISSS Task Force Revision DSG
Telefon	: +41 31 351 66 33 / +41 79 300 32 38
E-Mail	: ursula.widmer@widmer.ch
Datum	: 31. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.
2. Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.
3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Allgemein Sehr geehrte Damen und Herren ISSS bedankt sich für die Gelegenheit, im Rahmen der Vernehmlassung zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes Stellung nehmen zu können. Die Information Security Society Switzerland (ISSS; http://www.isss.ch) ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftlichen Aspekten von ICT-Sicherheit und Informationsschutz auseinander. ISSS ist offizieller ICT Security Fachpartner von SwissICT. **Die ISSS Stellungnahme beschränkt sich auf diejenigen Punkte, welche direkt oder indirekt im Zusammenhang mit der ICT-Sicherheit stehen. ISSS äussert sich daher nur zum Entwurf des Datenschutzgesetzes.** Die ICT-Sicherheit ist ein zentrales Anliegen des Datenschutzes. **Aus Sicht der ISSS und der von ihr vertretenen ICT Sicherheitsspezialisten ist die Sicherstellung der Kompatibilität der schweizerischen Datenschutzgesetzgebung mit derjenigen in der EU gemäss der neuen EU Datenschutzgrundverordnung von zentraler Bedeutung. Es wäre mit Rücksicht darauf, dass zahlreiche in der Schweiz domizilierte Unternehmen und Unternehmensgruppen mit Hauptsitz in der Schweiz sowohl dem schweizerischen als auch (für ihre Aktivitäten mit EU-Bezug) dem europäischen Datenschutzregime unterstellt sind, äusserst nachteilig, wenn in der Schweiz ohne zwingende Gründe Abweichungen zur EU geschaffen würden. Es würde dadurch nicht nur der im Hinblick auf die Wahrung des Datenschutzes und der Datensicherheit erforderliche Aufwand ohne zusätzlichen Nutzen und damit unnötig erhöht, sondern die Abweichungen zwischen den beiden Rechtsordnungen führen auch zu einer zusätzlichen Komplexität bei der Umsetzung der geforderten Massnahmen, was ein erhöhtes Risiko für die Sicherstellung des angestrebten Schutzniveaus bedeutet. Bereiche, in denen eine möglichst hohe Gleichläufigkeit der massgeblichen Regelungen anzustreben ist, sind z.B. die Anforderungen in Bezug auf die einzuhaltenden Standards betreffend die Datensicherheit, die Auftragsdatenbearbeitung, die Datenschutz-Folgeabschätzung sowie die Meldepflicht bei Datenschutzverletzungen.** Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und des Informationsschutzes im

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Datenschutzbereich der Schweiz leisten können und danken Ihnen für die Berücksichtigung unserer Anträge, welche wir Ihnen, wenn immer möglich, zu Ihrer Unterstützung gleich als ausformulierte Textvorlage mit dazugehöriger Begründung einreichen. An der ISSS Stellungnahme haben folgende ISSS Mitglieder mitgearbeitet (in alphabetischer Reihenfolge): Annino Umberto, Präsident ISSS, Infogurad AG; Bähler Konrad, Rechtsanwalt, Dr. Widmer & Partner, Rechtsanwälte; Breiting Petra, Informatikerin; Gammenthaler Daniel, Redguard AG; Hauser Ralf, PrivaSpehere AG; Hayoz Elmar, hayoz engineering gmbh; Jäschke Oliver, Swisscom AG; Keller Stefan, Informatiker; Lehmann Beat, Acting Counsel, Alcan Holding Switzerland AG; Rickenbacher Fridel, Partner, MIT-GROUP; Talleri Rocco, Rechtsanwalt, Talleri Law Studio Legale; Sidler Wolfgang, Inhaber, SIDLER Information Security GmbH; Widmer Ursula, Past President ISSS, Rechtsanwältin, Dr. Widmer & Partner, Rechtsanwälte; Zbinden Reto, CEO, Rechtsanwalt, Swiss Infosec AG Freundliche Grüsse Dr. Ursula Widmer, Rechtsanwältin, Past President ISSS / Leitung ISSS TaskForce Revision DSG.

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Verzicht auf den bDSB schwächt den Datenschutz **1 Einleitung** Der vorliegende Vorentwurf zum DSG (im Folgenden VE-DSG) enthält keine Verpflichtung von privaten Personen zur Ernennung einer spezifischen Funktion im Bereich Datenschutz. Daher kann in der vorliegenden Stellungnahme nicht auf einen entsprechenden Artikel Bezug genommen werden und die Ausführungen sowie Anträge erfolgen unter «Allgemeine Bemerkungen». Der Verzicht auf die im aktuellen Gesetz festgehaltene Funktion «Betrieblicher Datenschutzverantwortlicher», geregelt in Art. 11a DSG (*https://www.admin.ch/opc/de/classified-compilation/19920153/index.html#)* und konkretisiert in Art. 12a und Art. 12b VDSG (*https://www.admin.ch/opc/de/classified-compilation/19930159/index.html*), wird im erläuternden Bericht zum VE-DSG ohne weitere Begründungen nicht erwähnt und nicht erklärt. Obwohl auf europäischer Ebene eine Pflicht zur Einsetzung eines bDSB gilt, wird im VE-DSG ohne weitere Begründung auf eine solche verzichtet und gleichzeitig die Rechtsgrundlage für die über 1000 beim EDÖB gemeldeten bDSB entzogen. **Die Bezeichnung eines Betrieblichen Datenschutzbeauftragten (bDSB) stellt in der Praxis eine unabdingbare Grundvoraussetzung für die Umsetzung des Datenschutzes dar. Zudem kann und soll die Benennung eines bDSB die Verantwortlichen und Auftragsbearbeiter von verschiedenen Meldepflichten an den Beauftragten entlasten, aber auch den Beauftragten (EDÖB) von der Entgegennahme, Prüfung und Genehmigung dieser Informationen. Aufgaben des Beauftragten (EDÖB) werden so in die Unternehmen verlegt, die für den Datenschutz heikle Bearbeitungen durchführen. Wo immer möglich soll nicht der Staat für die Umsetzung von Rechtsvorschriften sorgen, sondern die dem Gesetz unterstellten Unternehmen durch interne organisatorische Regelungen. Administrative Leerläufe sind unbedingt zu verhindern. Mit der Beibehaltung und qualitativen und quantitativen Stärkung der Rolle des bDSB kann der Datenschutz gestärkt werden. Die Einsetzung von Datenschutzbeauftragten sollte seitens des Gesetzgebers und des EDÖB aktiv gefördert werden** **Zudem muss berücksichtigt werden, dass mit dem Verzicht auf die gesetzliche Verankerung die Rechtsgrundlage für die heute bereits eingesetzten Datenschutzbeauftragten - dringend notwendige Ressourcen für die Umsetzung der technischen und organisatorischen Massnahmen zum Schutz der elektronisch bearbeiteten Personendaten - entzogen würde, was auch zu einer Schwächung der gesamten Informationssicherheit führt.** Mit dem Verzicht auf die gesetzliche Verankerung eines bDSB würden in der Praxis wichtige Ressourcen für die Umsetzung des Datenschutzes verloren gehen (Art. 12b Abs. 2 lit. b DSG) welche sich auch mit der rasanten Entwicklung der Technik datenschutzrechtlich auseinanderzusetzen hatten (vgl. Ziele der Revision Ziff. 1.3 Bericht-VE).

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Die vorliegende Stellungnahme verwendet absichtlich den Begriff «Betrieblicher Datenschutzbeauftragter» zur Abgrenzung von den für die Einhaltung des Datenschutzes verantwortlichen Organe. Die aktuelle gesetzliche Bezeichnung als «Datenschutzverantwortlicher» ist diesbezüglich unbefriedigend und zu korrigieren. Die Notwendigkeit zur Einsetzung eines Datenschutzbeauftragten wurde auch von der **Europäischen Union** erkannt. Sie hat die Einsetzung eines Datenschutzbeauftragten in Art. 37 der Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 (im Folgenden **DSGVO**, *http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679*) aufgenommen. Der Verzicht auf die gesetzliche Verankerung eines bDSB im VE-DSG entspricht somit auch nicht der Stossrichtung der bereits in Kraft getretenen DSGVO, die nun bis zum 25. Mai 2018 durch alle Unternehmen in der EU umgesetzt werden muss und gemäss Geltungsbereich des Art. 3 DSGVO auch für bestimmte Schweizer Unternehmen Anwendung finden wird. Analog ist die Funktion des Datenschutzbeauftragten in Randziffer 63 Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 (im Folgenden Schengen-RL, *https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/eu-richtlinie-d.pdf*) ebenfalls ausdrücklich erwähnt. Es stellt sich die **Frage, inwieweit es sinnvoll ist, auf einen bDSB zu verzichten, obwohl dessen Funktion ausdrücklich in der DSGVO wie auch Schengen-RL vorgesehen ist und das Ziel der Revision u.a. darin liegt, sich der europäischen Entwicklung anzugleichen (Art. 1.3 Bericht-VE).** **2 Historische Entwicklung** Der «Betriebliche Datenschutzverantwortliche» ist seit der Revision des DSG im Jahr 2008 gesetzlich vorgesehen. In den Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz (*https://www.edoeb.admin.ch/datenschutz/00628/00784/index.html?lang=de&download=NHzLp-Zeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdXx4hGym162epYbg2c_JjKbNoKSn6A--*) äusserte sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zu den Gründen, die die Berufung eines bDSB empfehlenswert machen. Die Institution des «Datenschutzverantwortlichen» innerhalb eines Unternehmens oder einer öffentlichen Verwaltung existiere bereits in verschiedenen Ländern (namentlich Deutschland, Frankreich, den Niederlanden und Schweden) und werde nicht nur von den Datenschutzbehörden, sondern auch von den Unternehmen und den Verwaltungen, die sie eingeführt haben, positiv bewertet. Basierend auf der revidierten Fassung des DSG haben bis 27. Januar 2017 über 1000 Unternehmen ihren Betrieblichen

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Datenschutzverantwortlichen dem EDÖB formell gemeldet. **3 Internationaler Vergleich** **EU:** Die DSGVO sieht in Art. 37 klare Kriterien für die Notwendigkeit einer Ernennung eines Datenschutzbeauftragen vor. Insbesondere ist dies dann der Fall, wenn personenbezogene Daten, welche gemäss Schweizer Rechtsordnung in den Geltungsbereich der besonders schützenswerten Personendaten fallen, bearbeitet werden (Art. 3 lit. c VE-DSG und Art. 37 i.V.m. Art. 9 DSGVO). Die Wichtigkeit des Themas zeigt sich auch darin, dass die erste überhaupt publizierte Good Practice zur DSGVO gerade die Rolle und die Funktion dieser Datenschutzbeauftragten betraf (*http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf*). **Deutschland** wird gemäss Entwurf des Gesetzes zur Anpassung des Datenschutzrechts an die DSGVO sowie Schengen-RL (im Folgenden VE-DSAnpUG-EU, *http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutz-grundverordnung.html*) voraussichtlich die Anforderungen und die Verpflichtung zur Ernennung eines Datenschutzbeauftragten zusätzlich in seinen nationalen Gesetzen verschärfen. Gemäss Paragraph 38 des VE-DSAnpUG-EU **muss** der Verantwortliche und der Auftragsverarbeiter **eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennen**, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen oder verarbeiten sie personenbezogene Daten geschäftsmässig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie **unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen**. Weiter sollte gemäss Randziffer 63 der **Schengen-RL** der Verantwortliche eine Person benennen, die ihn dabei unterstützt, die interne Einhaltung der nach dieser Richtlinie erlassenen Vorschriften zu überwachen, es sei denn, ein Mitgliedstaat beschliesst eine Ausnahmeregelung für Gerichte und andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit. Mehrere Verantwortliche können dabei unter Berücksichtigung ihrer Organisationsstruktur und ihrer Grösse gemeinsam einen Datenschutzbeauftragten bestellen. Sodann ist zu berücksichtigen, dass im Kommentar zur **Revision der Europaratskonvention SEV 108** (*https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2*) gemäss Art. 8bis RZ 84 ausdrücklich auf die Einsatzmöglichkeit eines bDSB hingewiesen wird. Ein solcher betrieblicher Datenschutzbeauftragter könnte sowohl intern wie

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	auch extern eingesetzt werden und sollte der Behörde gemeldet werden (*«A possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a 'data protection officer' entrusted with the means necessary to fulfil his or her mandate. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller.»).* **4 Erkenntnisse der eingesetzten Begleitgruppe** Gemäss Ziff. 4.9.4 des Normkonzepts zur Revision des Datenschutzgesetzes vom 29. Oktober 2014 (*https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf*) kam die eingesetzte Begleitgruppe zum Schluss, dass die Eigenverantwortung der öffentlichen Datenbearbeitenden für die Einhaltung der datenschutzrechtlichen Vorschriften gestärkt und gefördert werden soll. Bei den Bundesorganen soll dabei (anstelle des heutigen «Beraters für den Datenschutz» gemäss Art. 23 VDSG) immer ein «Datenschutzverantwortlicher» im Sinne von Art. 12a und 12b VDSG, eingesetzt werden müssen (Ziff. 4.3.2). Für die Umsetzung in Unternehmen schlägt ein Teil der Begleitgruppe vor, ab einer bestimmten Grösse die Verpflichtung für den Einsatz eines «Datenschutzverantwortlichen» vorzusehen (Ziff. 4.3.2). Der Bundesrat könnte diese Verpflichtung auf kleinere Unternehmen ausweiten, bei denen ein erhöhtes Risiko besteht. Der Begriff «erhöhtes Risiko» wäre in der Botschaft, in der Verordnung oder in den Regeln der Guten Praxis bzw. in verbindliche Detailregeln (vgl. Ziff. 4.1.2 lit. b) zu präzisieren. Ein anderer Teil der Begleitgruppe ist der Meinung, dass die Verpflichtung zur Einsetzung eines bDSB nicht im Gesetz festgehalten werden solle. Stattdessen könne es den Regeln der Guten Praxis (vgl. Ziff. 4.1.2 lit. b) überlassen werden, je nach Unternehmen angemessene Mittel vorzusehen, um eine Datenbearbeitung zu gewährleisten, mit welcher den Rechten der betroffenen Personen Rechnung getragen wird (z.B. durch die Bestimmung eines Datenschutzverantwortlichen). Gemäss Ausführungen dieser Begleitgruppe bestehen jedoch keine Zweifel, dass bei den Bundesorganen ein «Datenschutzverantwortlicher» eingesetzt werden muss. Im VE-DSG fehlt ein solcher «Datenschutzverantwortlicher» bei den Bundesorganen wie auch für private Personen nun gänzlich. Den Anforderungen der Begleitgruppe wird in diesem Punkt somit nicht entsprochen. Bezgl. den unterschiedlichen Meinungen zum Einsatz eines Datenschutzverantwortlicher» in Unternehmen ist anzumerken, dass im Rahmen einer Verordnung keine Verschärfung des Gesetzes statthaft ist, insbesondere auch nicht in Regeln der Guten Praxis. Eine gesetzliche Verpflichtung zum

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Einsatz eines Datenschutzbeauftragten mit entsprechenden Erleichterungen bzw. Ausnahmen seitens Bundesrat/Verordnung ist hingegen zu empfehlen. **5 Notwendigkeit eines DSB in der Praxis** Aus Sicht der Praxis ist festzuhalten, dass die Verpflichtung zur formellen Bezeichnung einer für den Datenschutz zuständigen Stelle innerhalb eines Unternehmens die Umsetzung und die Güte der Datenschutzaktivitäten eindeutig positiv beeinflusst. Bereits mit dem Einsatz eines «betrieblichen Datenschutzverantwortlichen» gemäss Art. 11a Abs. 5 lit. e DSG wurde der Datenschutz gestärkt. Die Bezeichnung eines bDSB verbessert die Umsetzung der gesetzlich verankerten Grundsätze, die Berücksichtigung der Datenschutzanforderungen im Rahmen von Projekten und ermöglicht erst die Beantwortung offener Fragen zur Anwendung und Umsetzung des Datenschutzes. **Die Konzeption und Umsetzung der technischen und organisatorischen Massnahmen zum Schutz der elektronisch bearbeiteten Personendaten ist auch ein Teil der Aufgaben der mit der Informationssicherheit und der Datensicherheit beauftragten Stellen eines Unternehmens. In den meisten Fällen kann sich aber ausschliesslich der bDSB auf eine gesetzliche Grundlage und Notwendigkeit stützen. Innerhalb einer IT-Organisation und eines Unternehmens bestehen neben dem bDSB als Unterstützungs- und Überwachungsinstanz im gesamten Bereich der Informationssicherheit keine weiteren gesetzlich vorgesehenen Funktionen, ausser in speziell regulierten Bereichen. Die Tätigkeit eines bDSB fördert also die Güte und Qualität der Umsetzung der technischen und organisatorischen Massnahmen nicht nur bei der digitalen Bearbeitung von Personendaten, sondern darüber hinaus generell die Umsetzung der Anforderungen in den Bereichen der Informations- und Datensicherheit.** Die im Gesetz festgehaltenen Informationspflichten, Anforderungen an die Auftragsdatenbearbeitung, an die Sicherheit der Bearbeitung von Personendaten, die Informationspflichten, die Datenschutzfolgeabschätzung, die Meldung von Datenschutzverletzungen und die durch die Technik ermöglichten datenschutzfreundlichen Datenschutzeinstellungen können innerhalb eines Unternehmen nur dann wahrgenommen und umgesetzt werden, wenn es über eine entsprechend ausgeprägte Datenschutzorganisation verfügt. In der Praxis verfügen aber fast nur Grossunternehmen über entsprechende Ressourcen. **Ohne die Verpflichtung zur Einsetzung eines bDSB wird ein grosser Teil der Unternehmen auf die entsprechenden Ressourcen verzichten und den Handlungsbedarf im Bereich Datenschutz weder erkennen noch wahrnehmen.**

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Basierend auf dem geltenden Datenschutzrecht wurde bereits erreicht, dass über 1000 Unternehmen dem EDÖB die Einsetzung eines bDSB gemeldet haben. Diese würden ihren gesetzlichen Auftrag verlieren und der Datenschutz entsprechend geschwächt und nicht wie beabsichtigt gestärkt. **6 Fehlende Begründung** Unter Anbetracht der genannten Gründe erscheint es daher nicht nachvollziehbar, warum auf die gesetzliche Verankerung eines bDSB verzichtet werden soll. Insbesondere hätten die bestehenden Vorteile des geltenden Rechts berücksichtigt und allfällige Abweichungen ausführlich begründet werden müssen, was aber nicht erfolgt ist. Vergleicht man den VE-DSG mit dem VE-SEV 108, werden im VE-DSG u.a. Regelungen aufgenommen, welche vom VE-SEV 108 nicht gefordert werden (Daten Verstorbener [Art. 12 VE-DSG], kein datenschutzrechtliches Thema bei VE-SEV 108; zwingende Meldepflicht [Art. 6 Abs. 2 VE-DSG], jedoch ausschliesslich Meldepflicht auf Antrag gemäss Art. 12 Abs. 5 VE-SEV 108). Weiter werden Instrumente wie die Datenschutz-Folgeabschätzung (Art. 16 VE-DSG), Privacy by Design (Art. 18 Abs. 1 VE-DSG) und Privacy by Default (Art. 18 Abs. 2 VE-DSG) eingeführt, welche vom VE-SEV 108 nicht in dieser ausdrücklichen Art gefordert werden. Viel mehr dürften diese Instrumente direkt der DSGVO entnommen worden sein. Vor diesem Hintergrund ist es nicht ersichtlich, weshalb die gesetzliche Verankerung des bDSB überhaupt ohne weitere Begründung entfernt wurde. Insbesondere muss berücksichtigt werden, dass im Kommentar zur Revision der Europaratskonvention SEV 108 die Möglichkeit des Einsatzes eines bDSB zumindest genannt wird und mit dem Einsatz eines bDSB die Anforderungen nach Art. 8 Abs. 2 Entwurf SEV 108 umgesetzt werden könnten. **7 Anträge** Aufgrund dieser Überlegungen wird der Antrag gestellt, die Funktion des «Betrieblichen Datenschutzbeauftragten» im Datenschutzgesetz wie folgt zu berücksichtigen:

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Neuer Artikel 11bis: Bezeichnung eines Betrieblichen Datenschutzbeauftragten 1 Verantwortliche und Auftragsbearbeiter können einen Datenschutzbeauftragten bezeichnen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht. 2 Zur Bezeichnung eines Datenschutzbeauftragten sind verpflichtet a. Bundesorgane wenn sie Personendaten bearbeiten b. Auftragsbearbeiter wenn sie als wesentlicher Teil ihrer geschäftlichen Verrichtungen Personendaten für Verantwortliche bearbeiten c. Verantwortliche wenn sie zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet sind, oder wenn sie mehr als zehn Personen ständig mit der Bearbeitung personenbezogener Daten selbst oder über Dritte beschäftigen, oder wenn sie ohne gesetzliche Pflicht als wesentlicher Teil ihrer geschäftlichen Verrichtungen regelmässig 1 besonders schützenswerte Personendaten Dritter bearbeiten oder personenbezogenes Profiling betreiben; 2 Personendaten nicht bei der betroffenen Person beschaffen; 3 Personendaten an Dritte bekanntgeben; 4 Personendaten ins Ausland bekanntgeben; 5 Entscheidungen über Personen treffen, die ausschliesslich auf einer automatisierten Datenbearbeitung beruhen. 3 Der Datenschutzbeauftragte kann Arbeitnehmer des Verantwortlichen oder des Auftragsbearbeiters sein oder seine Aufgaben im Auftragsverhältnis erfüllen. 4 Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und dem Beauftragten mitzuteilen.

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	5 Der Bundesrat regelt Ausnahmen von der Pflicht zur Bestimmung eines Datenschutzbeauftragten, die Stellung und Aufgaben des betrieblichen Datenschutzbeauftragten sowie die Auswirkung seiner Bezeichnung auf die Einhaltung der Datenschutzschutzvorschriften. **Ergänzung in Art. 6 Abs. 2 Bekanntgabe ins Ausland in Ausnahmefällen (roter Text):** Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten oder dem Betrieblichen Datenschutzbeauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt. **Neuformulierung Art. 16 Abs. 3 Datenschutz-Folgeabschätzung (roter Text):** [3] Die Datenschutz-Folgeabschätzung und die vorgesehenen Massnahmen sind dem Beauftragten mitzuteilen oder in Zusammenarbeit mit dem Betrieblichen Datenschutzbeauftragten zu erarbeiten und dem Beauftragten im Rahmen einer Untersuchung oder auf dessen Aufforderung hin vorzulegen. Der Betriebliche Datenschutzbeauftragte kann dem Beauftragten die Datenschutz-Folgeabschätzung und die vorgesehenen Massnahmen zur Beurteilung unterbreiten. **Neuer Art. 17 Abs. 5 Meldung von Verletzungen des Datenschutzes (roter Text):** Verantwortliche und Auftragsbearbeiter treffen organisatorische und technische Massnahmen zur Feststellung der Ursache der Verletzung des Datenschutzes, zur Verhinderung künftiger Verletzungen bzw. zur Milderung ihrer möglichen nachteiligen Auswirkungen. Sie haben bei der Erfüllung ihrer Pflichten bei Verletzungen des Datenschutzes den Betrieblichen Datenschutzbeauftragten beizuziehen und dokumentieren alle Verletzungen des Schutzes personenbezogener Daten, deren Umstände und die ergriffenen Massnahmen.
	Strafrechtliches Sanktionen Regime Aus Sicht der ISSS ist das strafrechtliche Sanktionen Regime im EDSG weder akzeptabel noch zielführend. Die Fokussierung auf die einzelnen Mitarbeitenden birgt die Gefahr, dass sich kaum mehr geeignet qualifizierte Personen werden finden lassen, die Verantwortung mit Bezug auf den

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Datenschutz und die Datensicherheit zu übernehmen bereit sein werden, wenn sie ihre Tätigkeit unter den für einen einzelnen massiven Strafdrohungen gemäss den Art. 50 und 51 EDSG ausüben müssten. In der Praxis dürfte zwar oft schwierig sein, die konkrete Verantwortung einzelnen Personen zuzuweisen, da die Massnahmen betreffend Datenschutz und Datensicherheit das Ergebnis komplexer unternehmensinterner Prozesse darstellen. Dies würde dann zwar die einzelnen Mitarbeitenden entlasten und es käme Art. 53 EDSG zur Anwendung, welcher jedoch für Unternehmen eine Busse von maximal CHF 100'000 vorsieht. Dies ist jedoch eine zu geringe Strafdrohung, um einen präventiven Effekt auf die Entscheidprozesse innerhalb von Unternehmen in Richtung auf die Umsetzung wirksamer organisatorischer und technischer Massnahmen zur Wahrung des Datenschutzes und der Datensicherheit auszuüben. Die vorgesehene Regelung ist daher mit Bezug auf das Ziel der Sicherstellung des Datenschutzes kontraproduktiv, da sie einerseits auf der Ebene der einzelnen Mitarbeitenden abschreckend wirkt und die Übernahme von verantwortungsvollen Aufgaben im Bereich Datenschutz und Datensicherheit behindert und andererseits auf der Ebene der Unternehmen keinen massgeblichen Effekt haben wird. Die Regelung von Art. 52 betreffend die Verletzung der beruflichen Schweigepflicht entspricht demgegenüber im Grundsatz bisherigem Recht und vergleichbaren Geheimhaltungsvorschriften und kann in der vorgeschlagenen Form beibehalten werden. **Antrag:** Es ist mit Bezug auf Art. 50, 51 und 53 EDSG eine Angleichung an die Sanktionen Regelung gemäss der EU-DSBVO zwingend erforderlich.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
	DSG	2	2	a	Die Ausnahme der Datenbearbeitung zum rein persönlichen Gebrauch gemäss Art. 2 Abs. 2 lit. a EDSG ist grundsätzlich sinnvoll. Primär wird in diesem Zusammenhang an private Notizbücher und ähnliche Aufzeichnungen gedacht. Mit der verbreiteten Nutzung von Datenspeichern in der Cloud ist jedoch festzustellen, dass auch rein zum persönlichen Gebrauch bearbeitete Personendaten den gleichen Risiken, z.B. in Bezug auf unbefugte Zugriffe, ausgesetzt sind, wie Daten, welche nicht unter die Ausnahme von Art. 2 Abs. 2 lit. a EDSG fallen. Damit ist jedoch die Rechtfertigung der Ausnahme in Frage gestellt. Aus diesem Grund schlagen wir vor, die Ausnahme gemäss Art. 2 Abs. 2 lit. a EDSG wie folgt zusätzlich einzuschränken (roter Text): «… ausschliesslich zum persönlichen Gebrauch bearbeitet werden und hierbei keine Dienstleistungen Dritter in Anspruch nimmt.»
	DSG	6	2		**Antrag:** Ergänzung gemäss dem nachfolgend rot markierten Text (zur Begründung siehe oben Allgemeine Bemerkungen S. 9): Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten oder dem Betrieblichen Datenschutzbeauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.
	DSG	7	1bis (neu)		Im Hinblick auf die Bedeutung des zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiters abzuschliessenden Vertrages und die gegenseitigen Verantwortlichkeiten der beiden Vertragsparteien ist zu fordern, dass der Inhalt der getroffenen Vereinbarung inhaltlich nachweisbar ist.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					Antrag: Ergänzung von Art. 7 EDSG um den folgenden neuen Absatz 1bis (roter Text): 1bis Die Vereinbarung über die Auftragsdatenbearbeitung kann schriftlich oder in einer anderen Form abgeschlossen werden, welche den Nachweis durch Text ermöglicht.
	DSG	7	2		Es ist zu begrüssen, dass die weiteren Pflichten der Auftragsbearbeiter auf Verordnungsebene vom Bundesrat präzisiert werden sollen. Ergänzend ist festzuhalten, dass hierbei international anerkannte Normen und Standards zu berücksichtigen sind, wie z.B. die Norm ISO/IEC 27018 für Cloud Computing Anbieter. Weiter erscheint es sinnvoll, dass die Zielrichtung bezüglich der Regelung weiterer Pflichten zumindest angedeutet wird. **Antrag:** Ergänzung der Formulierung in Satz 2 von Art. 7 Abs. 2 wie folgt (roter Text): Der Bundesrat präzisiert, unter Berücksichtigung von internationalen anerkannten Standards, die weiteren Pflichten des Auftragsbearbeiters, insbesondere im Hinblick auf technische und organisatorische Massnahmen der Datensicherheit.
		8	1		Auch im Zusammenhang mit der Erarbeitung von Empfehlungen der guten Praxis sind international anerkannte Normen und Standards zu berücksichtigen, wie z.B. „ISO 27018 – CoP for protection of personally identifiable information (PII) in public clouds acting as PII processors“, „ISO 29100 – Privacy framework“, „ISO 29101 – Privacy Architecture framework“, “OECD Privacy and Security Guidelines”, “APEC Privacy Framework” etc., “Baustein 1.5 Datenschutz” des deutschen BSI sowie Controls Catalogues von Organisationen wie ISACA, CSA (Cloud Security Alliance), IAPP (International Association of Privacy Professionals) etc.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					Antrag: Ergänzung der Formulierung in Satz 1 von Art. 8 Abs. 1 wie folgt (roter Text): Der Beauftragte erarbeitet, unter Berücksichtigung von internationalen anerkannten Standards, Empfehlungen der guten Praxis, …. [Rest unverändert]
	DSG	11	1		Da die Definition von «Bearbeiten» in Art. 3 lit. d EDSG diesbezüglich nicht eindeutig ist, ist hier präzisierend festzuhalten, dass die Sicherheitsmassnahmen sich auch gegen den unbefugten Zugriff richten müssen. **Antrag:** Ergänzung von Satz 2 in Art. 11 Abs. 1 wie folgt (roter Text): Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten, unbefugten Zugriff und ~~oder~~ Verlust geschützt werden.
	DSG	11	2		Ebenfalls bei der Formulierung von Mindestanforderungen betreffend die Datensicherheit sind international anerkannte Normen und Standards zu berücksichtigen. **Antrag:** Ergänzung der Formulierung von Art. 11 Abs. 2 wie folgt (roter Text): Der Bundesrat erlässt, unter Berücksichtigung von internationalen anerkannten Standards, Bestimmungen über …. [Rest unverändert]
	DSG	11bis (neu)			**Antrag:** Ergänzung **eines neuen Art. 11bis** (zur Begründung siehe oben Allgemeine Bemerkungen S. 4ff):

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					Art- 11bis Bezeichnung eines Betrieblichen Datenschutzbeauftragten 1 Verantwortliche und Auftragsbearbeiter können einen Datenschutzbeauftragten bezeichnen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht. 2 Zur Bezeichnung eines Datenschutzbeauftragten sind verpflichtet a. Bundesorgane wenn sie Personendaten bearbeiten b. Auftragsbearbeiter wenn sie als wesentlicher Teil ihrer geschäftlichen Verrichtungen Personendaten für Verantwortliche bearbeiten c. Verantwortliche wenn sie zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet sind, oder wenn sie mehr als zehn Personen ständig mit der Bearbeitung personenbezogener Daten selbst oder über Dritte beschäftigen, oder wenn sie ohne gesetzliche Pflicht als wesentlicher Teil ihrer geschäftlichen Verrichtungen regelmässig 1 besonders schützenswerte Personendaten Dritter bearbeiten oder personenbezogenes Profiling betreiben; 2 Personendaten nicht bei der betroffenen Person beschaffen; 3 Personendaten an Dritte bekanntgeben; 4 Personendaten ins Ausland bekanntgeben;

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					5 Entscheidungen über Personen treffen, die ausschliesslich auf einer automatisierten Datenbearbeitung beruhen. 3 Der Datenschutzbeauftragte kann Arbeitnehmer des Verantwortlichen oder des Auftragsbearbeiters sein oder seine Aufgaben im Auftragsverhältnis erfüllen. 4 Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und dem Beauftragten mitzuteilen. 5 Der Bundesrat regelt Ausnahmen von der Pflicht zur Bestimmung eines Datenschutzbeauftragten, die Stellung und Aufgaben des betrieblichen Datenschutzbeauftragten sowie die Auswirkung seiner Bezeichnung auf die Einhaltung der Datenschutzschutzvorschriften.
	DSG	13	5		Der Begriff der „Speicherung“ von Daten ist unklar, da insbesondere bei der (automatisierten) Bearbeitung von Datenbeständen mit sogenannter „in-memory“ Technik keine Speicherung im herkömmlichen Sinn (persistente Speicherung) erfolgt, sondern eine flüchtige Speicherung – unter Umständen kann jedoch diese flüchtige Speicherung dennoch persistiert werden (für späteren Gebrauch, bei Speicherung eines „image“ einer virtuellen Maschine zum Zweck der Hochverfügbarkeit oder Backup etc.). Es ist ist daher eine Regelung vorzuziehen, analog Art. 14 Abs. 3 der EUDSGVO. Antrag: Art. 13 Abs. 5 EDSG ist wie folgt neu zu formulieren (roter Text): [5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person vom Verantwortlichen wie folgt informiert werden: a) unter Berücksichtigung der spezifischen Umstände der Berarbeitung der personenbezogenen Daten

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder, c) falls die Bekanntgabe an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Bekanntgabe.
	DSG	16			Modellhafte Datenschutz-Folgenabschätzungen für verbreitete Datenverarbeitungsszenarien, etwa beim Einsatz von Standardsoftware im CRM-Bereich, können als Grundlage von Datenschutzarchitekturen und Kontrollkatalogen in den Unternehmen dienen. In den verschiedenen Umsetzungen im Unternehmen könnten diese dann entsprechend der Vorgaben umgesetzt werden. Dadurch würde eine pragmatische, effiziente Umsetzung des DSG im Gleichklang mit den Erwartungen der EU-DGVSO ermöglicht. **Antrag**: Zulassung modellhafter Datenschutz-Folgenabschätzungen für verbreitete Datenverarbeitungsszenarien, etwa beim Einsatz von Standardsoftware im CRM-Bereich, auch als Grundlage von Datenschutzarchitekturen und Kontrollkatalogen in den Unternehmen.
	DSG	16	1		Im Gegensatz zu EU DSGVO Artikel 35 greift die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gemäss dem DSG Vorentwurf bereits bei einem voraussichtlich erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person. EU DSGVO Artikel 35 sieht eine solche Verpflichtung nur bei einem hohen Risiko für die Rechte und Freiheiten der Personen, sowie auf Grundlage von Positiv- und Negativlisten für eine Datenschutz-Folgenabschätzung Durchführung vor. – Hier wäre eine Angleichung wünschenswert, damit für jene Unternehmen in der Schweiz, für die sowohl das DSG als auch die EU-DSGVO zur Anwendung kommen, durch das DSG zumindest keine

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					zusätzlichen Datenschutz-Folgenabschätzungen erforderlich werden. **Antrag**: Angleichung des EDSG an die EU-DSGVO, damit für jene Unternehmen in der Schweiz, für die sowohl das DSG als auch die EU-DSGVO zur Anwendung kommen, durch das DSG zumindest keine zusätzlichen Datenschutz-Folgenabschätzungen erforderlich werden.
	DSG	16	1		Im Gegensatz zu EU DSGVO Artikel 35 nach dem nur der Verantwortliche eine Datenschutz-Folgenabschätzung durchführen muss, sind nach dem DSG Vorentwurf dazu der Verantwortliche oder der Auftragsbearbeiter aufgefordert. Für den Verantwortlichen und den Auftragsbearbeiter liegen hier offensichtlich keine gegenseitigen Informationspflichten oder Mitwirkungspflichten vor. Es ist unklar, wann eine konkrete Verpflichtung für eine der beiden Parteien vorliegt, bzw. ob eine erfolgte Datenschutz-Folgenabschätzung der einen Partei die andere von ihrer Verpflichtung entbindet. Es ist fraglich, ob ein Auftragsbearbeiter, der nicht zugleich Verantwortlicher ist, die Risiken für die Personen korrekt abschätzen kann, da er ggf. über keine Gesamtsicht verfügt. Dies könnte insbesondere bei Datenverarbeitungen unter Teilnahme mehrerer Auftragsbearbeiter zutreffen. Es ist unklar, ob die „vorgesehene Datenbearbeitung“, z.B. im Falle des Auftragsbearbeiters, auch den Einsatz einer bestehenden Datenbearbeitung durch diesen für einen neuen Zweck durch den Verantwortlichen umfassen würde. Prinzipiell wäre es wünschenswert, hier nur den Verantwortlichen in die Pflicht zu nehmen. **Antrag**: Streichung "oder der Auftragsbearbeiter"
	DSG	16	2		Im Gegensatz zu EU DSGVO Artikel 35, erlaubt DSG 16 (2) nicht explizit die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken im Rahmen einer einzigen Abschätzung. Dies führt im Vergleich zur EU zu höheren Aufwänden, sowohl innerhalb der Unternehmen als auch in der Abstimmung mit dem Beauftragten. Die Durchführung übergeordneter Datenschutz-

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					Folgenabschätzungen, und insbesondere auch die Wiederverwendung von Datenschutz-Folgenabschätzungen, die für den EU-Raum durchgeführt wurden, wären hier wünschenswert. Der vorliegende Text sollte überarbeitet werden, um übergreifende Datenschutz-Folgenabschätzungen, z.B. von Verarbeitungen innerhalb einer Gruppe von Unternehmen, zu ermöglichen (vgl. EU-DSGVO Art 36 (3) a). **Antrag**: Der vorliegende Text sollte überarbeitet werden um übergreifende Datenschutz-Folgenabschätzungen, z.B. von Verarbeitungen innerhalb einer Gruppe von Unternehmen, zu ermöglichen (vgl. EU-DSGVO Art 36 (3) a).
	DSG	16	2		Die Beschreibung der Datenschutz-Folgenabschätzung beinhaltet nicht die Würdigung der verbliebenen Risiken nach Umsetzung der vorgesehenen Massnahmen. Diese Beschreibung deckt nicht die notwendigen Inhalte einer EU-Datenschutz-Folgenabschätzung nach Art. 35 (7) ab. So fehlt z.B. eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck. **Antrag**: Angleichung der Inhalte der Datenschutz-Folgenabschätzung an die EU DSGVO

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
	DSG	16	3		Es bleibt offen, welche der beiden Parteien (Verarbeiter oder Auftragsbearbeiter) den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen berichtet. Es ist weiterhin unklar, ob die berichtende Partei die Datenschutz-Folgenabschätzung auch selbst durchgeführt bzw. die Massnahmen umgesetzt hat. **Antrag**: Streichung "oder der Auftragsbearbeiter"
	DSG	16	3		**Antrag:** Neuformulierung Art. 16 Abs. 3 Datenschutz-Folgeabschätzung gemäss dem nachfolgenden roten Text (zur Begründung vgl. oben S. 4ff., S. 11): [3] Die Datenschutz-Folgeabschätzung und die vorgesehenen Massnahmen sind dem Beauftragten mitzuteilen oder in Zusammenarbeit mit dem Betrieblichen Datenschutzbeauftragten zu erarbeiten und dem Beauftragten im Rahmen einer Untersuchung oder auf dessen Aufforderung hin vorzulegen. Der Betriebliche Datenschutzbeauftragte kann dem Beauftragten die Datenschutz-Folgeabschätzung und die vorgesehenen Massnahmen zur Beurteilung unterbreiten.
	DSG	16	3		Die Benachrichtigung erfolgt für jede durchgeführte Datenschutz-Folgenabschätzung, unabhängig von dem tatsächlich festgestellten Risiko. (Art. 16 1 erfordert eine Durchführung aufgrund eines voraussichtlich erhöhten Risikos.). EU-DSGVO Art. 36 legt im Vergleich dazu höhere Hürden. **Antrag**: Benachrichtigung nur bei Datenschutz-Folgenabschätzung mit einem tatsächlich festgestellten hohen Risiko.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
	DSG	16	4		Es ist unklar, welcher der beiden Parteien (Verarbeiter oder Auftragsbearbeiter) der Beauftragte ggf. seine Einwände mitteilt, und ob diese zur gegenseitigen Information verpflichtet sind. Falls beide Parteien unabhängig voneinander Datenschutz-Folgenabschätzungen eingereicht haben, könnte es in der Praxis zu Inkonsistenzen bei deren Beurteilung kommen. **Antrag**: Streichung "oder dem Auftragsbearbeiter"
	DSG	17	1		Da die Definition von «Bearbeiten» in Art. 3 lit. d EDSG diesbezüglich nicht eindeutig ist, ist hier präzisierend festzuhalten, dass die Informationspflicht auch bei unbefugten Zugriffen gilt. Es ist weiter zu bedenken, dass es Situationen gibt, insbesondere bei sogenannten DDoS-Attacken, in denen nicht auf Daten zugegriffen wird, in denen aber die Daten den Berechtigten für die ordentliche Bearbeitung nicht mehr oder nur mit Einschränkungen verfügbar sind, was ebenfalls zu Beeinträchtigungen der Persönlichkeit von betroffenen Personen führen kann. Es rechtfertigt sich daher, die Informationspflicht auf entsprechende Ereignisse zu erweitern. **Antrag:** Ergänzung von Art. 17 Abs. 1 wie folgt (roter Text): Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung, einen unbefugten Datenzugriff, ~~oder~~ den Verlust von Daten oder eine nicht bloss sehr kurzfristige rechtswidrige Verhinderung oder Einschränkung der rechtmässigen Bearbeitung von Daten, ….. der betroffenen Personen.
	DSG	17	4		Die Information über meldepflichtige Ereignisse ist häufig sensitiver Natur. Der Auftragsbearbeiter hat daher berechtigte Geheimhaltungsinteressen des Verantwortlichen zu wahren, denn es liegt in der Verantwortung des letzteren, wie er den Informationspflichten gemäss Abs. 1-3 nachkommen will. Zudem muss sich die Informationspflicht gemäss Abs. 4 auf die gleichen Ereignisse beziehen, wie sie

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					in Art. 1 erwähnt werden, sofern sich diese beim Auftragsbearbeiter ereignen: **Antrag:** Art. 17 Abs. Abs. 4 ist wie folgt zu ergänzen (roter Text): Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung, einen unbefugten Datenzugriff, den Verlust von Daten oder eine nicht bloss sehr kurzfristige rechtswidrige Verhinderung oder Einschränkung der rechtmässigen Bearbeitung von Daten. Er beachtet hierbei die berechtigten Geheimhaltungsinteressen bei der Wahl und der Form der Information.
	DSG	17	5 (neu)		Antrag: Ergänzung eines neuen Absatz 5 gemäss dem nachfolgenden roten Text (zur Begründung siehe S. 4ff., S. 11) [5] Verantwortliche und Auftragsbearbeiter treffen organisatorische und technische Massnahmen zur Feststellung der Ursache der Verletzung des Datenschutzes, zur Verhinderung künftiger Verletzungen bzw. zur Milderung ihrer möglichen nachteiligen Auswirkungen. Sie haben bei der Erfüllung ihrer Pflichten bei Verletzungen des Datenschutzes den Betrieblichen Datenschutzbeauftragten beizuziehen und dokumentieren alle Verletzungen des Schutzes personenbezogener Daten, deren Umstände und die ergriffenen Massnahmen.
	DSG	18	3 (neu)		Es erscheint sinnvoll, wenn auch im Zusammenhang mit den Massnahmen der Privacy by Design und der Privacy by Default, wie sie gemäss Abs. 1 und 2 von Art. 18 EDSG vorgesehen werden, auf Verordnungsebene unter Berücksichtigung von international anerkannte Normen und Standards eine Präzisierung durch den Bundesrat erfolgt, ähnlich wie z.B. bei Art. 7 Abs. 2 oder Art. 11 Abs. 2 EDSG. Wichtig ist hierbei, dass die Anforderungen international, insbesondere mit denjenigen in der EU, konform sind. **Antrag:** Ergänzung der Formulierung von Art. 18 um einen neuen Abs. 3 mit folgendem Wortlaut (roter

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
					Text): [3] Der Bundesrat erlässt, unter Berücksichtigung von internationalen anerkannten Standards, Bestimmungen über die Mindestanforderungen an die Massnahmen gemäss oben Abs. 1 und 2.
	DSG	50-55			Ausgleichung an EU-DSGVO. Siehe dazu oben die detaillierten Ausführungen und Anträge unter Allgemeine Bemerkungen S. 11f.
	DSG	59			Grammatikfehler: „.. müssen die ~~für~~ Verantwortlichen sowie die~~der~~ Auftragsbearbeiter.“ **Antrag**: Korrektur gemäss roter Markierung.

Amstutz Jonas BJ

Von: Bürki Peter <peter.buerki@buerki-bolt.ch>
Gesendet: Mittwoch, 5. April 2017 09:33
An: Amstutz Jonas BJ
Betreff: Vernehmlassung
Anlagen: D0231110.docx

Freundlicher Gruss

Ärztegesellschaft
des Kantons St. Gallen
lic. iur. Peter Bürki
Rechtskonsulent
Auerstrasse 2
9435 Heerbrugg

G: +41 71 727 97 87
F: +41 71 727 97 88

Email: peter.buerki@buerki-bolt.ch

Stellungnahme von

Name / Firma / Organisation	Äerztegesellschaft des Kantons St. Gallen
Abkürzung der Firma / Organisation	KAeG SG
Adresse	Äerztegesellschaft des Kantons St. Gallen Brenner treuhand Gewerbestr. 6 9242 Oberuzwil
Kontaktpersonen	Dr. med. Jürg Lymann lic. iur. Peter Bürki
Telefon	081 736 14 34 (Lymann) 071 727 97 87 (Bürki)
E-Mail	juerg.lymann@srrws.ch peter.buerki@buerki-bolt.ch
Datum	: 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	Die Ärztegesellschaft des Kantons St. Gallen ist die Vereinigung der frei praktizierenden und der angestellten Ärztinnen und Ärzte in freier Praxis und in den Spitälern, soweit diese im Kanton St. Gallen wohnen oder beruflich tätig sind. Wir haben ca. 1500 Mitglieder. Die KAeG SG setzt sich gemäss ihren Statuten für die beruflichen, standespolitischen und wirtschaftlichen Belange ihrer Mitglieder ein. Sie fördert die fachliche Qualifikation ihrer Mitglieder für eine gute und effiziente ärztliche Versorgung und Gesundheitspflege der Bevölkerung und orientiert sich dabei an anerkannten Regeln von Ethik, Recht, Wissenschaft und Wirtschaftlichkeit. Unsere Ärztinnen und Ärzte mit eigener Praxis oder als Mitarbeitende von Gemeinschaftspraxen und auch die Ärztinnen und Ärzte in unseren Spitäler sind für die breite Bevölkerung die primären Ansprechpartner in Gesundheitsfragen. Sie sind für Patientinnen und Patienten Vertrauenspersonen. Letztere offenbaren den behandelnden Ärztinnen und Ärzte wichtige Informationen über die eigene Person und die eigene Gesundheit. Zugleich gelangen ärztliche Fachpersonen als Teil ihrer Tätigkeit, z. B. im Rahmen der Anamnese und der Diagnose, zu wesentlichen Informationen über den physischen oder psychischen Gesundheitszustand einer Person. Es ist daher offensichtlich, dass datenschutzrechtliche Problemstellungen im Zusammenhang mit der ärztlichen Tätigkeit eine ganz zentrale Bedeutung einnehmen. Die Ärzteschaft ist sich dessen bewusst. Das Arztgeheimnis ist ein zentrales Instrument, um die Interessen der Patientinnen und Patienten an der Vertraulichkeit von Informationen über die eigene Person zu schützen. Die Verpflichtungen der Ärzteschaft, das Arztgeheimnis zu schützen und zu achten ist unabdingbarer Bestandteil einer erfolgreichen und vertrauensbasierten ärztlichen Tätigkeit. Dafür setzt sich die KAeG SG permanent und mit Nachdruck ein. Das Arztgeheimnis und damit auch der Schutz der Privat- und Intimsphäre der Patientinnen und Patienten ist zugegebenermassen stark gegenläufigen Tendenzen ausgesetzt. Der technisch medizinische Fortschritt und die immer ausgeprägtere Spezialisierung innerhalb der Ärzteschaft verlangt immer stärker einen Austausch von Daten innerhalb der ambulant tätigen Ärzteschaft, aber auch zwischen Ärzten und Spitälern, Apotheken etc. Je integrierter die Gesundheitsversorgung ist, desto wichtiger wird der Austausch von Patientendaten. Dabei handelt es sich vielfach um sensible Daten. Dazu kommt aber auch ein finanzielle Aspekt. Die Versicherer verlangen im Rahmen der Wirtschaftlichkeitsprüfungen zunehmend detaillierte Angaben über ärztliche Behandlungen von bestimmten Patienten. Diesem Datenhunger der Versicherer kommt der Datenhunger der öffentlichen Hand durchaus gleich. Art. 30 ff. KVV verlangt von den Leistungserbringern, und damit auch von den freipraktizierenden Ärztinnen und Ärzte die Bekanntgabe wesentlicher Daten über die eigene Tätigkeit. Was die Patientendaten anbelangt, so erfolgt die Weitergabe auf anonymisierter Basis. Demgegenüber sind die Ärztinnen und Ärzte verpflichtet, gegenüber dem Bundesamt für Statistik wesentliche Angaben über die eigene Geschäftstätigkeit offen zu legen. Insoweit gibt es für die freipraktizierende Ärzte-

	schaft gegenüber dem Staat keinen absoluten Datenschutz. Datenschutzfragen im Gesundheitswesen sind nicht nur aus der Patientenperspektive zu beleuchten. Vielmehr ist auch der Perspektive der Leistungserbringer Rechnung zu tragen. Deren Rechte und Pflichten verlangen einen adäquaten Schutz. Weiter möchten wir darauf hinweisen, dass die freipraktizierende Ärzteschaft aus Gründen der Effizienz sowie der Konzentration auf die Kerntätigkeit immer stärker einzelne administrative Tätigkeiten ausgelagert hat, so insbesondere das Rechnungswesen. Auch dies führt dazu, dass Daten der Arztpraxen, aber auch von einzelnen Patienten von Dritten bearbeitet werden. Die Dokumentation und Informationspflichten der freipraktizierenden Ärzteschaft sind in den letzten Jahren ganz erheblich erweitert worden. Dies führt dazu, dass die Belastung der Ärzteschaft durch diese Art der Tätigkeit finanziell und zeitlich erheblich zugenommen hat. Es gibt angesichts dessen auch eine Grenze der Zumutbarkeit, was den Aufwand in administrativer Hinsicht anbelangt. Diesbezüglich ist insbesondere dem Verhältnismässigkeitsprinzip Rechnung zu tragen. Die Grundanliegen Ihres Entwurfes sind unbestritten, nämlich: Die möglichst weitgehende, wenn auch nicht zwingend vollständige Harmonisierung der schweizerischen Datenschutzgesetzgebung mit den europäischen Vorgaben, die Verbesserung des Datenschutzes natürlicher Personen in ausgewählten Aspekten. Verschiedenste Aspekte des Gesetzes sind positiv zu würdigen, wie nachfolgend bei der Kommentierung einzelner Bestimmungen des Vorentwurfes aufgezeigt werden wird. Es gibt allerdings auch Aspekte, welche für die freipraktizierende Ärzteschaft weniger vorteilhaft sind. Dazu zählen nebst einigen Unklarheiten mit Bezug auf die möglichen Auswirkungen auf die freipraktizierende Ärzteschaft vor allem die Befürchtung einer weiteren Zunahme der administrativen Belastung und die erhebliche Verschärfung sowie Erweiterung des Strafrahmens. Dies ändert allerdings nichts daran, dass die KAEG SG dem Vorhaben einer Totalrevision des DSG grundsätzlich positiv gegenübersteht. Es wird aber nicht einfach sein, dies unseren Mitgliedern, für die die Arbeit am und mit den Patientinnen und Patienten im Vordergrund steht, im positiven Sinne zu kommunizieren. Gerade deshalb wünschen wir, dass den Anliegen der Ärzteschaft, wie sie in der nachfolgenden Kommentierung zum Ausdruck kommt, Rechnung getragen wird.
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)					
Name/Firma	**Gesetz**	**Art.**	**Abs.**	**Bst.**	**Bemerkung/Anregung**
KAEG SG	DSG	1			Das neue Gesetz schliesst den Schutz der Persönlichkeit und der Grundrechte von juristischen Personen nicht mehr in den Gesetzeszweck ein. Dagegen ist im Grundsatz nichts einzuwenden. In der Tat unterschied sich diesbezüglich, mit dem stark erweiterten, auch auf juristische Personen bezogenen Schutzbereich die schweizerische Gesetzgebung von den vergleichbaren Rechtsnormen in der EU sowie in anderen Staaten. Aus Sicht der KAEG SG ist entscheidend, dass weiterhin auch dann die Daten natürlicher Personen geschützt sind, wenn diese im Besitze juristischer Personen sind und von diesen bearbeitet werden. Was die Ärzteschaft als Leistungserbringer anbelangt, so sind auch frei praktizierende Ärztinnen und Ärzte, welche Einzelfirmen sind, weiterhin vom Gesetz geschützt. Dies ist demgegenüber offensichtlich nicht mehr der Fall bei als juristische Körperschaften organisierten Leistungserbringern. Dies ist in Kauf zu nehmen.
KAEG SG	DSG	2			Art. 2 bestimmt den Geltungsbereich des Gesetzes. Es ist klar und auch völlig richtig, dass ärztliche Leistungserbringer, d. h. also Ärztinnen und Ärzte sowie als juristische Personen organisierte ärztliche Leistungserbringer Patientendaten bearbeiten und daher vom Gesetz erfasst werden. Problematisch ist indessen, dass das Gesetz keinerlei Regelungen trifft, was das Verhältnis zu anderen Gesetzen anbelangt. Im Gesundheitsbereich kann dies ein ernsthaftes Problem sein. Die Abgrenzungen sind bei weitem nicht eindeutig. Das Bundesgesetz über das elektronische Patientendossier EPDG und das KVG enthalten wichtige, auch datenschutzrechtlich relevante Bestimmungen. Im welchem Verhältnis stehen diese Normen zum neuen DSG? Die Fragestellung ist alles andere denn banal. Denn gemäss dem Gesetzesentwurf sind die Sanktionen schärfer als unter dem geltenden Recht. Es ist daher für die ärztlichen Leistungserbringer von erheblicher Bedeutung zu wissen, ob die speziellen Regelungen in den genannten Gesetzen vorgehen, im Übrigen aber die Bestimmungen des DSG gelten, oder ob mit den Regelungen in den Spezialgesetzen die Geltung des DSG generell ausgeschlossen wird. Aus Sicht der Ärzteschaft ist eine entsprechende Klärung mehr als wünschbar. Dies muss nicht zwingend in Art. 2 geschehen. Die derzeitige Gesetzesvorlage spricht sich indessen generell zu diesem zentralen

					Problem nicht aus. Aus Sicht der Ärzteschaft stellt dies eine wesentliche, mit grossen Rechtsunsicherheiten verbundene Unterlassung dar.
KAEG SG	DSG	3			Was die grundsätzlich sehr wünschbaren Definitionen in Art. 3 anbelangt, so sind aus Sicht der ambulant tätigen Ärzteschaft vor allem die Bestimmungen zu den besonders schützenswerten Personendaten sowie zum Profiling relevant. Es bedarf keiner näheren Erläuterung, dass Daten über die Gesundheit besonders schützenswert sind. Es ist auch klar, dass diese Qualifikationen zu erhöhten Sorgfaltspflichten führt, welche im Gesetz näher ausgeführt sind. Was das Profiling anbelangt, so sei der Hinweis erlaubt, dass die ärztliche Tätigkeit häufig, wenn nicht zumeist auch in einem Profiling bezüglich des Gesundheitszustandes besteht. Mit anderen Worten: Ärztinnen und Ärzte müssen sich an die Regelungen halten, welche im Gesetz sich auf das Profiling beziehen, insbesondere an die damit verbundenen erhöhten Sorgfaltspflichten. Nun ist eigentlich das Profiling auf andere Konstellationen bezogen: Nämlich auf das Sammeln und Verbinden von Daten über eine Person ohne deren Einwilligung, um von dieser Person ein Profi zu gewinnen. Diese Konstellation unterscheidet sich erheblich vom Profiling im Rahmen des Gesundheitswesens bzw. von ambulant tätigen Ärztinnen und Ärzten. Denn dort findet das Profiling freiwillig und mit der ausdrücklichen oder zumindest konkludenten Zustimmung der Patientinnen und Patienten statt. Es stellt sich daher ganz ernsthaft die Frage, ob sich eine Anwendung der strengeren Bestimmungen zum Profiling auf die Ärzteschaft rechtfertigt. Zu denken ist z. B. an das Profiling in Notfällen oder bei psychischen Erkrankungen. Dies gilt im Übrigen auch für die Umschreibung des Begriffes des Verantwortlichen bzw. des Auftragsbearbeiters. Sind ärztliche Leistungserbringer, ist der in freier Praxis tätige Arzt Verantwortlicher im Sinne von Art. 3 lit. h DSG? Es ist wohl davon auszugehen. Jede Krankheitsgeschichte stellt eine Bearbeitung in einer Art und Weise dar, dass der Bearbeitende ein Verantwortlicher ist. Ist dies im Gesundheitsbereich wirklich sachgerecht?
KAEG SG	DSG	4			Aus Sicht der KAEG SG ist gegen die allgemeinen Bestimmungen bzw. gegen die allgemeinen Grundsätze grundsätzlich nichts einzuwenden. Allerdings ist auf Probleme hinzuweisen, welche sich aus einer Anwendung von Art. 4 Abs. 6 im Arzt – Patientenverhältnis ergeben können. Nach dieser Bestimmung ist die ausdrückliche Einwilligung einer Person bei besonders schützenswerten Personendaten und beim Profiling erforderlich. Mithin bestehen erhöhte Anforderungen an das Einverständnis. Im Grundsatz ist dagegen nichts einzuwenden. Indessen stösst dies an Grenzen. Wie steht es in Notfällen oder bei psychischen Erkrankungen, welche die Urteils-

					und Handlungsfähigkeit einer Person in Frage stellen? In welchem Verhältnis steht die Regelung von Art. 4 Abs. 6 zu den Regelungen im EPDG? Was geschieht, wenn eine Patientin, wenn ein Patient diese Einwilligung verweigert, und es dadurch für die Ärztin oder den Arzt schwierig wird, die Anamnese vorzunehmen und eine geeignete Heilmethode vorzuschlagen? Wie sieht dies mit der Haftung des Arztes bzw. der Ärztin aus? Resultiert aus der fehlenden Einwilligung von Patientinnen und Patienten ein Selbstverschulden? Daraus ergibt sich, dass erhebliche, wichtige und nicht wenige Fragen offen sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	5			Keine Bemerkungen
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	6			Diese Bestimmung kann vor allem relevant sein bei Notfällen im Ausland. In einem solchen Fall kann unter Umständen die betroffene Person nicht einwilligen. Trotzdem kann es zum Schutz ihrer Gesundheit unabdingbar sein, dass Gesundheitsdaten in ein Land transferiert werden, das nicht dasselbe Schutzniveau hat wie die Schweiz. Art. 6 Abs. 1 Bst. d sieht völlig zu Recht die Möglichkeit vor, dass Personendaten ins Ausland bekannt gegeben werden können, wenn das Leben oder die körperliche Unversehrtheit bei der betroffenen Person in Frage steht. Es ist davon auszugehen, dass es immer auch dann der Fall ist, wenn ein Gesundheitsproblem vorliegt. Völlig unnötig ist aus Sicht der ambulant tätigen Ärzteschaft demgegenüber, dass in solchen Fällen der Beauftragte informiert werden muss. Nach Ansicht der KAEG SG handelt es sich hier um einen Fall, bei welchem Empfehlungen der guten Praxis durch die Branche selber auszuarbeiten sind. Wie sich aus dem Kommentar zu Art. 8 DSG ergibt, ist die KAEG SG der Auffassung, dass derartige Empfehlungen der guten Praxis unter gesetzlich definierten Umständen auch von den allgemeinen gesetzlichen Regelungen abweichen können (vgl. nachfolgend zu Art. 8), wenn sie vom Beauftragten genehmigt worden sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	7			Diese Bestimmung ist im Gesundheitsbereich von erheblicher Bedeutung, werden doch oft Patientendaten im Auftrag von Leistungserbringer oder aufgrund einer gesetzlichen Anordnung von Dritten bearbeitet. Was die ambulant tätige Ärzteschaft anbelangt, so ist insbesondere die Rechnungsstellung und der Inkasso durch Unternehmungen wie z. B. die Ärztekasse zu erwähnen.

					Im Gesundheitsbereich wirft die an sich sinnvolle Bestimmung zwei Fragen auf, die unklar bleiben: Gemäss Art. 7 Abs. 1 gilt diese Bestimmung auch für den Fall einer Übertragung der Bearbeitung von Personendaten gestützt auf ein Gesetz. Wie ist dies zu verstehen? Bedeutet dies, dass überall dort, wo das Gesetz von Leistungserbringern verlangt (insbesondere das KVG), Daten zu liefern, Art. 7 zur Anwendung gelangt? Z. B. im Geltungsbereich des EPDG? Der KAEG SG scheint diese Bestimmung in soweit unklar zu sein. Art. 7 Abs. 1 Bst. b) spricht gesetzliche Geheimhaltungspflichten an. Dazu gehört selbstverständlich auch das Arztgeheimnis. Bedeutet dies, dass eigentlich die Auftragsdatenbearbeitung für Leistungserbringer im Gesundheitswesen, insbesondere für ambulant tätige Ärztinnen und Ärzte unzulässig ist? Eine solche Auffassung würde auf jeden Fall völlig den Gepflogenheiten widersprechen. Zur Klärung der Verhältnisse wäre es zu begrüssen, wenn Art. 7 Abs. 1 eine Ziffer c. angefügt würde, welche wie folgt lauten kann: "Wenn die betroffene Person der Bearbeitung ihrer Personendaten durch einen Auftragsbearbeiter zustimmt." Diese Präzisierung würde wohl erheblich mehr Klarheit bringen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	8			Art. 8 ist eine interessante, grundsätzlich begrüssenswerte Bestimmung. Dies gilt insbesondere für das dort vorgesehene Konzept der regulierten Selbstregulierung. Grundsätzlich ist es zu begrüssen, wenn der Beauftragte auf dem Wege der Empfehlung Datenschutzvorschriften konkretisieren kann. Die Rechtsnatur dieser Empfehlung ist aber teilweise nicht klar. Mit Recht wird zwar in Art. 9 Abs. 2 darauf hingewiesen, dass die Datenschutzvorschriften auch auf andere Weise eingehalten werden können, als in Empfehlungen der guten Praxis vorgesehen ist. Die Empfehlungen sind mithin nicht umfassend rechtsverbindlich. Mit ihrer Einhaltung ist indessen klar, dass auch die Datenschutzvorschriften eingehalten werden. Insoweit ist trotz allem von einer limitierten Rechtsverbindlichkeit auszugehen. Dies bedeutet, dass Art. 8 praktisch eine Delegation von Rechtsetzungsbefugnissen an den Beauftragten enthält. Angesichts dessen wäre es wünschbar, wenn konkretisiert würde, unter welchen Voraussetzungen der Beauftragte Empfehlungen der guten Praxis erlassen soll. Denn es ist wohl davon auszugehen, dass die Verwaltungs- und Gerichtspraxis sich sehr stark an diesen Empfeh-

					lungen orientieren werden. Faktisch wird es so sein, dass in Bereichen, in denen eine Empfehlung besteht, deren Nichteinhaltung im Sine einer wiederlegbaren Vermutung eine Verletzung von Datenschutzvorschriften darstellt. Abs. 2 ist grundsätzlich inhaltlich zu begrüssen, aber nach Ansicht der KAEG SG noch zu wenig konkret. So ist z. B. nicht klar, in welcher Form verantwortliche und interessierte Kreise die Empfehlungen des Beauftragten ergänzen können. Werden solche Ergänzungen ebenfalls gemäss Abs. 3 veröffentlich? Unklar ist sodann was unter "interessierte Kreise" zu verstehen ist. Im Gesundheitsbereich gibt es Akteure mit wiederstreitenden Interessen: die Leistungserbringer, die Versicherer, die Patienten und der Staat. Können sie alle je eigene Empfehlungen der guten Praxis erlassen? Wer prüft die Legitimation dieser "interessierten Kreise"? Wie legitimieren sich diese? Grundsätzlich ist sehr zu befürworten, wenn z. B. Branchenverbände eigene Empfehlungen der guten Praxis erarbeiten können. Diese Verbände verfügen über ein grosses know-how, denn ihre Arbeit ist von ausgeprägter Sachnähe geprägt. Indessen kann die Gefahr widersprechender Empfehlungen der guten Praxis nicht ausgeschlossen werden. Diese Gefahr kann nur durch eine Genehmigung der Empfehlungen durch den Beauftragten ausgeschlossen werden. Allerdings verlangt dies, wie nachfolgend zu zeigen sein wird, eine Präzisierung in Art. 9 Abs. 1. Was die Genehmigung anbelangt, so erfolgt diese durch den Beauftragten, falls die Empfehlungen eines Verantwortlichen oder interessierter Kreise mit dem Datenschutzvorschriften vereinbar sind. Es stellt sich allerdings die Frage, ob es nicht möglich sein sollte, unter gesetzlich umschriebenen Voraussetzungen und im Sinne einer Ausnahme auch Empfehlungen zu genehmigen, welche in nicht zentralen Bereichen der Datenschutzgesetzgebung von einzelnen Normen abweichen, weil der Gehalt der Empfehlung besser den Bedürfnissen und Gepflogenheiten einer Branche entspricht als die starren Regelungen des Datenschutzrechtes. Die KAEG SG ist der Auffassung, dass dies näher zu prüfen ist. Gerade der Gesundheitsbereich weist z. B. sehr spezifische, auch widersprüchliche Bedürfnisse unter dem Gesichtswinkel des Datenschutzes auf. Es sollte z. B. möglich sein, in einzelnen Bereichen vom Erfordernis der ausdrücklichen Zustimmung, welches sonst bei besonders schützenswerten Daten gilt, abzuweichen. Hierfür könnte eine Empfehlung, genehmigt vom Beauftragten, genügen. Die Veröffentlichung von Genehmigungen ist zwingend erforderlich, führt doch deren Einhaltung dazu, dass die entsprechenden Datenschutzvorschriften eingehalten werden. Als in dem Sinne

					verbindliche Konkretisierung von einzelnen Bereichen der Datenschutzgesetzgebung muss eine Veröffentlichung erfolgen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	9			Vgl. hierzu auch die Bemerkungen zu Art. 8. Die Rechtsnatur der Empfehlungen ist unklar. Sie sind wohl am ehesten Verwaltungsverordnungen vergleichbar. Das Besondere daran ist, dass auch Empfehlungen privater bzw. "interessierter Kreise" im Fall der Genehmigung verbindliche Kraft haben können. Abs. 1 von Art. 9 hält nun allerdings ganz generell fest, dass ein Verantwortlicher die Datenschutzvorschriften einhält, wenn er die Empfehlung der guten Praxis befolgt, welche die entsprechenden Datenschutzvorschriften konkretisieren. Dies ist insoweit erstaunlich, als dass dies offensichtlich auch für nicht genehmigte Empfehlungen der guten Praxis interessierter Kreise, ja theoretisch sogar für Empfehlungen der guten Praxis Privater, welche der Beauftragte mangels Kompatibilität mit der Datenschutzgesetzgebung nicht genehmigt hat, gelten kann. Dies kann mit Sicherheit nicht die Meinung von Art. 9 Abs. 1 DSG sein. Die Bestimmung ist daher entsprechend zu ergänzen, dass dies nur für genehmigte Empfehlungen der guten Praxis gelten kann. Die KAEG SG begrüsst sodann Abs. 2 von Art. 9. Dieser Absatz verdeutlicht, dass Empfehlungen nicht vollumfänglich rechtsverbindlich sein können.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	12			Art. 12 betrifft die ambulant tätige Ärzteschaft in doppelter Hinsicht: Wegen des kostenlosen Einsichtsrechts und wegen der Aufweichung des Berufsgeheimnisses. Jede Ärztin, jeder Arzt besitzt besondere schützenswerte Daten der Patientinnen und Patienten, dies namentlich auch in der Form der Krankengeschichte. Stirbt ein Patient oder eine Patientin, stellt sich die Frage des Umgangs mit diesen Daten insbesondere dann, wenn Dritte, namentlich Erben, Einblick in die Daten verlangen. Derzeit gilt, dass das Arztgeheimnis Ärztinnen und Ärzte dazu verpflichtet, im Grundsatz die Privatsphäre ihrer ehemaligen Patientinnen und Patienten, die verstorben sind, zu achten, es sei denn, eine Güterabwägung würde zu einem anderen Resultat führen. Diese Regelung schützt das Arztgeheimnis und vor allem auch die Rechte der Patientinnen und Patienten. Art. 12 will das bisher existierende Regel/Ausnahmeverhältnis ins Gegenteil verkehren, dies zumindest bei Ehepartnern, Partner einer eingetragenen Partnerschaft und bei Nachkommen: Sofern die verstorbene Person nicht ausdrücklich die Einsicht untersagt hat, ist der Arzt, ist die Ärztin als Verantwortliche verpflichtet, einen entsprechenden Einblick zu gewähren.

					Die KAEG SG ist der Auffassung, dass das Regel-Ausnahmeverhältnis nicht umgekehrt werden sollte, denn eigentliche Missstände sind nicht bekannt. Der Arzt soll weiterhin die Interessen seines verstorbenen Patienten, seiner verstorbenen Patientin wahren können. Insbesondere der Umstand, dass bei bestimmten Kategorien ein schutzwürdiges Interesse vermutet wird, führt nach Auffassung der KAEG SG zu erheblichen Schwierigkeiten. Bei gewissen Diagnosen, insbesondere im psychiatrischen Bereich, kann die vorgeschlagene Regelung zu sehr fragwürdigen Resultaten führen. Es geht hier auch um den postmortalen Persönlichkeitsschutz. Es steht einem Patienten offen, dem Arzt gegenüber zu erklären, dass im Falle seines Todes Verwandte und/oder die Nachkommen Einblick z. B. in die Krankengeschichte nehmen können. Das Arztgeheimnis und die Interessen der Patienten gebieten es indessen, dass das Geheimnis die Regel, die Bekanntgabe die Ausnahme sein soll.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13-16			Die Bedeutung dieser Bestimmungen für ambulant tätige Ärztinnen und Ärzte ist unklar. Es ist wohl davon auszugehen, dass Ärztinnen und Ärzte grundsätzlich Verantwortliche im Sinne des vorgeschlagenen neuen Datenschutzgesetzes sind. Die konkreten Auswirkungen sind indessen nicht absehbar. Die ausgedehnten Informationspflichten sind auf jeden Fall aus Sicht der KAEG SG im Verhältnis zwischen ambulant tätigen Ärztinnen und Ärzten und ihren Patienten dem ärztlichen Behandlungsverhältnis nicht angemessen. Die KAEG SG ist der Auffassung, dass sich die Ermächtigung zur Beschaffung von Personendaten und deren Weiterleitung als Teil der medizinischen Behandlung aus dem Behandlungsverhältnis ergibt. Es scheint zumindest, dass Informationspflichten, und zwar ausdrückliche, dann bestehen, wenn ein Grundversorger den Patienten an einen Spezialisten überweist, sodann im Verhältnis zwischen Belegarzt und Spital, möglicherweise bei der Behandlung eines Falles in einem Medical Board etc. Dies ist nicht erforderlich. Art. 13 ff. sind daher Beispiele von Regelungen, welche im Gesundheitsbereich in Empfehlungen der guten Praxis zumindest teilweise relativiert werden sollten. Dies setzt allerdings voraus, dass der Beauftragte in einem Genehmigungsentscheid von der Beachtung einzelner Bestimmungen des DSG dispensieren kann. Vergleiche hierzu auch die Stellungnahme zu Art. 8 DSG. Ähnliche Vorbehalte wie zu den Artikeln 13-15 ergeben sich bei Art. 16. Bedeutet die Bestimmung, dass sämtliche ambulant tätige Ärztinnen und Ärzte eine Datenschutz-Folgenabschätzungt vornehmen müssen? Aufgrund des Wortlautes von Art. 16 muss man davon ausgehen, zumal Ärztinnen und Ärzte in den Besitz besonders schützenswerter Daten ihrer Patientinnen und Patienten gelangen. Die Risiken und möglichen Folgen dürfen indessen bei den meisten

					Ärztinnen und Ärzte gleich sein. Die geforderte Folgenabschätzung gemäss Art. 16 Abs. 2 würde daher bei den meisten Ärztinnen und Ärzte genau gleich aussehen und wäre damit nicht mehr als die rein formale Erfüllung einer lästigen Pflicht, nicht aber eine echte Information. Vollends keinen Sinn macht in diesem Zusammenhang die Benachrichtigungspflicht an den Datenschutzbeauftragten. Abschliessend ist festzuhalten, dass die Bestimmung, zumindest was deren potentielle Anwendung im Gesundheitsbereich anbetrifft, völlig unklar ist und überdies potentiell einen erheblichen Aufwand verursachen kann. Dies gilt insbesondere für die ambulant tätige Ärzteschaft. Auch bei Art. 16 handelt es sich um eine Bestimmung, deren Einhaltung und Umsetzung bei der ambulant tätigen Ärzteschaft wohl erheblich zu relativieren ist, dies auf dem Wege von Empfehlungen der guten Praxis.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19			Diese Bestimmung zählt ebenfalls zu den Normen, deren Reichweite für die ambulant tätige Ärzteschaft völlig unklar ist. Ein Hausarzt ist Verantwortlicher im Sinne des Gesetzes. In seiner Funktion muss er immer wieder Patientendaten an Dritte weitergeben (Versicherer, Vertrauensarzt, Spital, Spezialist, etc.). Ist ernsthaft die Meinung, dass er in jedem Fall die Empfängerinnen und Empfänger von Daten über die Patienten im Sinne von Art. 19 Bst. b) zu informieren hat? Aus Sicht der KAEG SG macht dies keinen Sinn.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	23			Art. 23 umschreibt die Persönlichkeitsverletzungen in einer Art und Weise, welche ambulant tätige Ärztinnen und Ärzte als Verantwortliche unmittelbar betrifft: Es ist unmittelbar mit der ärztlichen Tätigkeit verbunden, wenn Dritten als Teil der Behandlung besonders schützenwerte Personendaten bekannt gegeben werden. Ebenso findet, z. B. in einer Krankengeschichte ein Profiling statt. Geht man vom Wortlaut von Art. 23 Abs. 2 aus, so würde praktisch immer eine Persönlichkeitsverletzung vorliegen. Dies kann nicht Sinn der Bestimmung sein, zumindest nicht mit Bezug auf die normale berufliche Tätigkeit ambulant tätiger Ärztinnen und Ärzte. Die Rechtfertigungsgründe gemäss Art. 24 ändern an diesem Befund nur wenig.
Fehler! Verweisquelle konnte nicht	DSG	24			Die Problematik liegt vor allem an den Anforderungen mit Bezug auf die Einwilligung der Patientinnen und Patienten. Die ärztliche Tätigkeit wird auf jeden Fall sehr stark behindert, wenn jeweils immer ausdrückliche Einwilligungen einzuholen sind. Auch hier zeigt sich wieder der alte

gefunden werden.					Konflikt: Einerseits sind Gesundheitsdaten besonders schützenswerte Daten, auf der anderen Seite verlangen die Umstände, insbesondere der Gesundheitszustand von Patientinnen und Patienten, häufig, dass diese Daten weitergegeben werden, dies im Interesse des Behandlungserfolgs oder auch bei der Rechnungsstellung. Zu kritisieren ist sodann die Umschreibung "möglicherweise" in Art. 24 Abs. 2. Damit wird das Vorliegen von Rechtfertigungsgründen relativiert und eine Rechtsunsicherheit geschaffen. Entweder liegt ein Rechtfertigungsgrund vor oder nicht. So wie Abs. 2 von Art. 24 jetzt formuliert ist, wissen Datenbearbeiter nicht, ob sie nun Daten zulässigerweise bearbeiten oder die Persönlichkeit Betroffener verletzen. Mit der Formulierung werden nur Rechtstreitigkeiten gefördert. Zu beachten sind in diesem Zusammenhang auch die verschärften Strafbestimmungen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	26-36			Die besonderen Bestimmungen für die Datenbearbeitung durch Bundesorgane im 6. Abschnitt des Gesetzesentwurfes sind für die ambulant tätige Ärzteschaft nicht unmittelbar relevant. Allerdings sind sie sonst im Gesundheitswesen von erheblicher Bedeutung, handelt es sich doch um Bestimmungen, an welche sich die Krankenversicherer in Vollzug des KVG bzw. im Vollzug der Grundversicherung zu halten haben. Ferner – dies darf nicht übersehen werden – bearbeiten Bundesorgane, eben zum Beispiel die Krankenversicherer, aber auch das BAG und weitere Bundesämter die wirtschaftlichen Daten der frei praktizierenden Ärztinnen und Ärzte als Leistungserbringer. Mit Bezug auf letzteres möchte die KAEG SG klar festhalten, dass nach ihrer Auffassung nie ein öffentliches Interesse daran besteht, die finanziellen Daten einzelner in freier Praxis tätiger Ärztinnen und Ärzte zu veröffentlichen. Dies gilt auch für das grundsätzliche Recht, Name, Vorname, Adresse und Geburtsdatum einer Person gestützt auf Art. 29 Abs. 4 des Gesetzentwurfs bekannt zu geben. Zumindest völlig voraussetzungslos darf dies nicht geschehen. Auch in einem solchen Falle muss ein legitimes Interesse an der Bekanntgabe bzw. an die Kenntnisnahme dieser Daten bestehen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	37-49			Die ambulant tätige Ärzteschaft wird durch die neuen Bestimmungen zum eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten nicht unmittelbar bzw. nicht besonders betroffen. Ungeklärt ist indessen aus Sicht der KAEG SG das Verhältnis zwischen den Untersuchungsmassnahmen gemäss Art. 41 des Gesetzesentwurfs und die Geltung des Arzt- bzw. Patientengeheimnisses. Die KAEG SG geht davon aus, dass auch im Falle von Untersuchungen, welche

					sich gegen eine einzelne Ärztin bzw. gegen einen einzelnen Arzt richten, dieser sich auf das Arztgeheimnis berufen kann. Wäre dem anders, so müsste dies ausdrücklich im Gesetz geregelt sein. Die KAEG SG wäre gegen eine solche Regelung.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	50-55			Der Entwurf sieht eine massive Ausweitung der strafrechtlichen Sanktionen im Vergleich zur geltenden Regelung in Art. 34 und 35 DSG vor. Die RL (EU) 2016/680 vom 27. April 2016, also die neue Datenschutzlinie der EU verlangt solches nicht. Sie hält in Art. 57 unter dem Titel "Sanktionen" allein fest: Die Mitgliedstaaten legen fest, welche Sanktion bei einem Verstoss gegen die nach dieser Richtlinie erfassten Vorschriften zu verlängern sind, und treffen die zu deren Anwendung erforderlichen Massnahmen. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein.“ Das ist alles. Der Entwurf regelt demgegenüber in sechs, zum Teil umfangreichen Artikel die strafrechtlichen Sanktionen. Die KAEG SG ist der Auffassung, dass ein derart umfangreicher Strafkatalog nicht erforderlich ist. Überdies sind die Strafnormen zum Teil wenig präzise abgefasst bzw. können Anlass geben für unnötige, auch belastende Strafverfahren. Klar handelt es sich zu einem erheblichen Teil um Antragsdelikte. Dies ändert aber nichts daran, dass ein Strafverfahren eingeleitet werden kann, dies mit den möglichen Folgen für die Betroffenen. Strafrechtlich verfolgt werden können gemäss dem Entwurf private Personen, was juristische und natürliche Personen einschliesst. Allerdings ist die Möglichkeit der Bestrafung juristischer Personen gestützt auf Art. 53 des Entwurfes eingeschränkt und nur möglich, wenn der Bussenbetrag CHF 100'000.- nicht überschreitet und die Ermittlung der verantwortlichen natürlichen Person unverhältnismässig wäre. Es bleibt abzuwarten, was insbesondere letztere Umschreibung zu bedeuten haben wird. Auf jeden Fall ergibt sich aus den vorgeschlagenen Gesetzesnormen, dass die strafrechtliche Verantwortung natürlicher Personen die Regel und die Möglichkeit der Bestrafung juristischer Personen die Ausnahme darstellen soll. Dies bedeutet insbesondere, dass auch einzelne Ärztinnen und einzelne Ärzte sich strafbar machen können. Mithin sind die Strafbestimmungen für die ambulant tätige Ärzteschaft von erheblicher Bedeutung, ist doch auf deren Tätigkeit – wie bereits gesehen – das DSG grundsätzlich anwendbar.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	50			Die fehlende Präzision der vorgeschlagenen Strafnormen zeigt sich bereits bei Art. 50 Abs. 1. Die Erteilung einer unvollständigen Auskunft kann mit Busse bis zu CHF 500'000.- bestraft wer-

					den. Wann ist eine Auskunft unvollständig? Auch eine eventual vorsätzlich begangene unvollständige Auskunft führt zur Bestrafung. Die Abgrenzungsprobleme sind programmiert. Dieselbe Problematik ergibt sich auch bei der Verletzung von Informationspflichten. Ein gutes Beispiel einer wirklich missglückten Strafnorm ist die in Art. 50 Abs. 1 lit. e vorgesehene Möglichkeit einer Bestrafung mit Busse bis zu CHF 500'000.-, dies nicht nur auf Antrag, bei der Unterlassung, dem Beauftragten Verletzungen des Datenschutzes nach Art. 17 Abs. 1 zu melden. Art. 17 Abs. 1 sieht eine Meldepflicht vor bei einer unbefugten Datenbearbeitung oder beim Verlust von Daten, macht dann aber einen Vorbehalt, dies für den Fall, dass ein Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person "voraussichtlich" ausbleibt. Es muss also nicht immer in jedem Fall gemeldet werden, vielmehr kann eine Abwägung vorgenommen werden. Es macht keinen Sinn, derartige Normen mit einer strafrechtlichen Sanktionsmöglichkeit zu versehen. In vielen Fällen genügt es, anstelle einer strafrechtlichen Drohung dem Beauftragten die Möglichkeit zu geben in der Sache zu verfügen und die Nichteinhaltung der Verfügung mit StGB Art. 292 abzusichern. Auch die in Art. 51 des Entwurfes vorgesehenen Strafmöglichkeiten bei Verletzungen von Sorgfaltspflichten können ohne weiteres durch Verfügungen des Beauftragten ersetzt werden, welche mit StGB Art. 292 abgesichert werden können, sollte dies erforderlich sein. Nach Ansicht der KAEG SG muss der Katalog der Strafnormen nochmals umfassend überdacht werden. Von diesem Katalog wären vor allem Personen betroffen, welche in Unternehmungen für den Datenschutz verantwortlich sind. Die Strafnormen sind derart unpräzise und weit gefasst, dass derartige Personen auch angesichts der Komplexität von Datenschutzfragen insbesondere im Gesundheitsbereich ein hohes Risiko laufen, in Strafverfahren verwickelt zu werden. Die KAEG SG erachtet dies als nicht sinnvoll.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG				

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen	
Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten	
Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht	

gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"		
Name/Firma	**Art.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
3003 Bern

Per Mail: jonas.amstutz@bj.admin.ch

Brüttisellen, 31. März 2017

Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz: Stellungnahme der KARTAC

Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Mit diesem Schreiben nehmen wir Bezug auf die am 21. Dezember 2016 eröffnete Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) und die Änderung weiterer Erlasse. Wir bedanken uns in diesem Zusammenhang für die Möglichkeit zur Stellungnahme, von der wir gerne Gebrauch machen.

Die Interessengemeinschaft der Zahlkartenindustrie KARTAC bezweckt die Interessenvertretung und Meinungsbildung ihrer Mitglieder[1] gegenüber anderen Vereinigungen, Firmen, Institutionen, Gesetzgeber und der Öffentlichkeit zur Wahrung der Interessen der Zahlkartenindustrie. Die Mitglieder sind Herausgeber von physischen und digitalen Charge-, Debit-, Kredit- und Prepaidkarten sowie von Kundenkarten mit Zahlfunktion sowie Organisationen, die im Namen und Auftrag von Kartenherausgebern die Issuing-Funktion wahrnehmen.

Die KARTAC hat den Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) und die Änderung weiterer Erlasse in enger Abstimmung mit der Swiss Payment Association (SPA) geprüft und vertritt weitgehend die identischen Ansichten wie sie in der SPA Stellungnahme vom 04. April 2017 vorzufinden sind.

---

[1] Mitglieder der KARTAC sind per März 2017 folgende Unternehmen: Accarda AG, BonusCard.ch AG, CCC Credit Card Center AG, Cembra Money Bank AG, Cornèr Bank AG, Magazine zum Globus AG, MF Group AG, Möbel Pfister AG, PayRed Card Services AG, paysafecard.com Schweiz GmbH, PostFinance AG, Swiss Bankers Prepaid Services AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Card Services SA.

Management Summary

Wettbewerbsfähigkeit stärken und Chancen der Digitalisierung nutzen
Die zentralen Anliegen nach Förderung der Wettbewerbsfähigkeit der Schweizer Wirtschaft, Gewährleistung des freien Verkehrs personenbezogener Daten und Chancennutzung im Bereich der Digitalisierung nimmt der VE-DSG nicht auf. Er fokussiert einseitig auf den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen. Damit missachtet er einerseits die Tatsache, dass das Recht auf Schutz der personenbezogenen Daten kein absolutes Recht ist, sondern dass es gegen andere Grundrechte abgewogen werden muss. Andererseits leistet der VE-DSG keinen Beitrag zur Stärkung der wirtschaftlichen Wettbewerbsfähigkeit und hilft nicht, die Chancen der fortschreitenden Digitalisierung zu nutzen. Der Gesetzesvorschlag ist daher grundlegend neu auszurichten.

Prinzipien und Selbstverantwortung ins Zentrum der Regulierung stellen
Wenn im Gesetz vom „Verantwortlichen" gesprochen wird, dann soll der Gesetzgeber diesem auch (Eigen-)Verantwortung übertragen. In der Konsequenz heisst das z.B., dass der Verantwortliche nicht mit einer Vielzahl von Genehmigungs- und Meldepflichten überzogen werden soll. Zudem ist prinzipienbasiert (und nicht regelbasiert) zu legiferieren, sodass den Rechtsunterworfenen Raum für eine effiziente und effektive Regulierungsumsetzung verbleibt.

Kein Swiss Finish
Gegenüber dem internationalen Datenschutzniveau ist kein Swiss Finish vorzunehmen. Einerseits ist ein solcher für die angestrebte Äquivalenz mit dem europäischen Datenschutzniveau nicht erforderlich, anderseits würde er die Schweizer Wirtschaft bzw. deren internationale Wettbewerbsfähigkeit ungebührlich belasten. Darüber hinaus ist eine zusätzliche Kostenbelastung Schweizer Unternehmen zu befürchten, wenn für Inlandskunden und EU-Auslandskunden abweichende Prozesse und Regelungen implementiert werden müssten; hierdurch würde die Wettbewerbsfähigkeit Schweizer Unternehmen zusätzlich ungerechtfertigt belastet werden. Des Weiteren würde ein Swiss Finish unverhältnismässig in die fragile Balance zwischen zweckmässiger bzw. notwendiger Datenbearbeitung und legitimem Datenschutz eingreifen.

Abstimmung zwischen Datenschutzgesetz und Aufsichtspraxis der FINMA
Für Finanzintermediäre bestehen mit dem sich derzeit in Überarbeitung befindlichen FINMA-Rundschreiben 2008/7 (Outsourcing Banken) und mit Anhang 3 zum FINMA-Rundschreiben 2008/21 (Operationelle Risiken Banken) bereits weitreichende Vorgaben zum Outsourcing und zum Umgang mit elektronischen Kundendaten. Diese Vorgaben dürfen durch die Neufassung des Datenschutzgesetzes nicht weiter verschärft werden, und es darf auch nicht zu Redundanzen oder Widersprüchen in der praktischen Umsetzung der verschiedenen Vorgaben kommen

Die Begriffsbestimmung „Profiling" enger fassen
Die in Art. 3 lit. f. VE-DSG vorgesehene Profiling-Definition umfasst (im Gegensatz zur EU-Regulierung) auch die Verarbeitung nicht-personenbezogener Daten sowie die nicht-automatisierte Auswertung von Daten. Zudem wird der Anwendungsbereich nicht auf das Profiling der Daten einer bestimmten betroffenen Person eingeschränkt. Der Wortlaut umfasst somit auch die Auswertung von anonymen Daten und potenziell auch die Auswertung hinsichtlich der Merkmale von Personengruppen. Das führt deutlich zu weit und würde zu einschneidenden Einschränkungen und neuen Risiken in der Datenbearbeitung für Unternehmen führen.

Es ist deshalb davon Abstand zu nehmen. Dies umso mehr, als sich aus einer engeren Begriffsbestimmung kein erhöhtes Risiko für die Persönlichkeit der betroffenen Person ergibt.

Keine ausdrückliche Einwilligung für das Profiling
In Art. 4 Abs. 6 VE-DSG soll generell eine ausdrückliche Einwilligung für das Profiling statuiert werden. Dafür gibt es keine Rechtfertigung, womit darauf zu verzichten ist.

Verankerung eines Rechtfertigungstatbestands für das Profiling
Für Zahlungsdienstanbieter sind Datenbearbeitungen, inklusive Profiling, insbesondere zur Bekämpfung von Betrug und zur Erhöhung der Sicherheit unverzichtbar – und das gleichermassen im Interesse der Konsumentinnen/Konsumenten und Händler wie der Zahlungsdienstleister. Dabei müssen die Datenbearbeitungen/Profile regelmässig den neuesten Bedrohungen und veränderten Bedingungen angepasst und entsprechend weiterentwickelt werden können. Eine Rechtfertigung dieser Datenbearbeitungen muss daher weiterhin ohne ausdrückliche Einwilligung und gestützt auf ein überwiegendes Interesse zulässig sein. Alles andere wäre unpraktikabel und würde die effiziente und effektive Betrugsbekämpfung unnötig beeinträchtigen. Art. 24 Abs. 2 VE-DSG ist deshalb um einen entsprechenden Rechtfertigungstatbestand zu ergänzen.

Informationspflicht bei der Beschaffung von Personendaten

Für Unternehmen ist es zur Wahrung ihrer berechtigten Interessen erforderlich, dass Personendaten auch aus Drittquellen (z.B. Wirtschaftsauskunfteien oder Marketingdatenbanken) bezogen sowie von diesen Drittquellen erhoben, verarbeitet und bereitgestellt werden, um z.B. Kreditprüfungen oder die Allokation von Werbemitteln effektiv, fokussiert und effizient durchführen zu können. Die in Art. 13 Abs. 5 VE-DSG vorgesehene Informationspflicht gegenüber der betroffenen Person im Hinblick auf die Beschaffung von Personendaten aus Drittquellen ist unverhältnismässig, nicht praktikabel und beeinträchtigt unverhältnismässig die berechtigten Interessen der Schweizer Unternehmen. Auf sie ist daher zu verzichten.

Vorkehrungen gegen den Missbrauch des Auskunftsrechts der betroffenen Person
Dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke – wie kostenlose Beschaffung von Beweismitteln oder querulatorische Begehren – ist auf Gesetzesebene entgegenzuwirken. Die vorgesehene generelle Kostenlosigkeit der Auskunft ist daher durch das grundsätzliche Prinzip eines angemessenen Unkostenbeitrag zu ersetzen (Art. 20 Abs. 1 VE-DSG). Weiter ist in Art 21 VE-DSG als weitere Rechtfertigung zur Einschränkung des Auskunftsrechts diejenige aufzunehmen, dass das Auskunftsersuchen im Kern nicht datenschutzrechtlichen Zwecken dient (Rechtsmissbrauch).

Kein genereller Entzug der aufschiebenden Wirkung bei Beschwerden gegen vorsorgliche Massnahmen
Dass Beschwerden gegen vorsorgliche Massnahmen generell keine aufschiebende Wirkung haben sollen, ist unverhältnismässig. Vorsorgliche Massnahmen können für die Betroffenen mit erheblichem Schadenspotenzial verbunden sein. Ein Verantwortlicher muss sich gegen ein unverhältnismässiges Vorgehen in jedem Verfahrensstadium wirksam zur Wehr setzen können. Art. 44 Abs. 3 VE-DSG ist daher zu streichen.

Verzicht auf strafrechtliche Sanktionen
Strafrechtliche Sanktionen sind für die Äquivalenz zum europäischen Datenschutzniveau in keiner Weise erforderlich – im Gegenteil: Sie dürften sich punkto Äquivalenz als hinderlich erweisen, da die DSGVO zur Durchsetzung das verwaltungsrechtliche Verfahren vorsieht.

Darüber hinaus ist die Androhung strafrechtlicher Sanktionen – erst Recht persönlicher strafrechtlicher Sanktionen – unverhältnismässig und in hohem Masse kontraproduktiv. Ganz besonders stossend ist dabei die Strafbarkeit von fahrlässigen DSG-Verstössen. Hinzu kommt, dass viele der sanktionierten DSG-Bestimmungen – zu Recht – weniger regel- und eher prinzipienbasiert konzipiert sind. Prinzipienbasierte Normen eignen sich jedoch nicht dafür, mit strafrechtlichen Sanktionen verknüpft zu werden, da für die Rechtsunterworfenen unter strafrechtlichen Gesichtspunkten zu wenig klar eingegrenzt ist, welches Verhalten mit Strafe bedroht ist (nulla poena sine lege stricta). Auf die Artikel 50 bis 55 VE-DSG ist daher zu verzichten.

Keine zusätzlichen Präzisierungen der Pflichten des Auftragsbearbeiters durch den Bundesrat
In Art. 7 Abs. 2 VE-DSG soll der Bundesrat verpflichtet werden, die weiteren Pflichten des Auftragsbearbeiters zu präzisieren. Dafür gibt es – neben den gesetzlichen Regeln und den vertraglichen Vereinbarungen zwischen Verantwortlichem und Auftragsbearbeiter – keine Notwendigkeit und keinen Raum.

Keine Information der betroffenen Person über Identität und Kontaktdaten der Auftragsbearbeiter
Gemäss Art. 13 Abs. 4 VE-DSG hätte der Verantwortliche die betroffene Person über die Identität und die Kontaktdaten der Auftragsbearbeiter zu informieren. Das wäre in der Praxis unverhältnismässig aufwändig bzw. würde die Geschäftsprozesse stark behindern bis verunmöglichen. Zudem ginge es über das EU-Datenschutzniveau hinaus. Und das ohne Grund: Denn entscheidend ist für die betroffene Person nicht, dass sie den Auftragsbearbeiter kennt, sondern dass die Bearbeitung ihrer Daten unter Einhaltung der gesetzlichen Vorgaben erfolgt. Dies sicherzustellen ist Gegenstand von Art. 7 VE-DSG. Art. 13 Abs. 4 VE-DSG ist deshalb zu streichen.

Keine gesetzliche Verpflichtung zu Datenschutz-Folgenabschätzungen
Zur Einhaltung der komplexen Bestimmungen des Datenschutzgesetzes basiert ein Unternehmen bereits heute laufend auf fachkundigen Analysen und Beurteilungen sowie darauf abgestützten Massnahmenpaketen. Derartige Grundvoraussetzungen für die Rechtsumsetzung – wie das Durchführen einer Datenschutz-Folgenabschätzung – gesetzlich zu verankern, bringt keinen Mehrwert, sondern verursacht allein zusätzliche Bürokratie, Zeitverluste und Rechtsunsicherheit – letzteres insbesondere in Zusammenhang mit der Konsultationspflicht beim Beauftragten. Art. 16 VE-DSG ist daher zu streichen.

1. Grundsätzliche Ausführungen

1.1 Prinzipien und Selbstverantwortung ins Zentrum der Regulierung stellen

Wir anerkennen die Notwendigkeit, mit der Totalrevision des Datenschutzgesetzes ein Datenschutzniveau herzustellen, das äquivalent zum europäischen Schutzniveau ist und so den reibungslosen grenzüberschreitenden Datenverkehr gewährleistet. Wichtig ist aus unserer Warte, dass die erforderliche Äquivalenz über eine prinzipienbasierte Regulierung – und nicht eine regelbasierte – hergestellt wird, welche Raum für praxisnahe, effiziente und effektive Lösungen lässt, die innerhalb des gesteckten Rahmens von den regulierten Akteuren selbstverantwortlich entwickelt werden können. Dieses auf eine lange und erfolgreiche Tradition zurückblickende Schweizer Regulierungskonzept darf nicht verlassen werden, denn es

trägt ganz wesentlich zur Verträglichkeit der Schweizer Gesetzgebung und zur internationalen Wettbewerbsfähigkeit der Schweizer Volkswirtschaft bei. Wenn im Gesetz vom „Verantwortlichen" gesprochen wird, dann soll der Gesetzgeber diesem auch zutrauen, dass er seine (Eigen-)Verantwortung wahrnimmt. Konkret heisst das zum Beispiel, dass der Verantwortliche nicht mit einer Vielzahl von Genehmigungs- und Meldepflichten überzogen werden soll. **Die KARTAC setzt sich deshalb für eine prinzipienbasierte Regulierung ein, welche den Regulierten Selbstverantwortung belässt.**

1.2 Kein Swiss Finish

Nebst dieser Grundanforderung ist es genau so wichtig, dass gegenüber dem internationalen Datenschutzniveau kein Swiss Finish vorgenommen wird. Einerseits ist ein solcher für die angestrebte Äquivalenz mit dem europäischen Datenschutzniveau unnötig, anderseits würde er die Schweizer Wirtschaft bzw. deren internationale Wettbewerbsfähigkeit ungebührlich belasten. Zudem würde ein Swiss Finish unverhältnismässig in die fragile Balance zwischen zweckmässiger bzw. notwendiger Datenbearbeitung und legitimem Datenschutz eingreifen. **Die KARTAC lehnt daher Swiss-Finish-Normen ab und beantragt, konsequent auf solche zu verzichten** (siehe dazu die nachfolgenden Ausführungen zu den einzelnen Themen). Dort, wo europäische Normen über das Ziel hinausschiessen, soll der Schweizer Gesetzgeber auch den Mut haben, diese nicht nachzuahmen, sondern eine angemessene Schweizer Lösung zu implementieren. Das gilt ganz besonders dort, wo solche Normen zur Erreichung der Äquivalenz nicht erforderlich sind.

1.3 Wettbewerbsfähigkeit stärken und Chancen der Digitalisierung nutzen

Gemäss Erläuterungsbericht soll das neue Datenschutzgesetz die Wettbewerbsfähigkeit der Schweiz erhalten und stärken, indem ein Umfeld geschaffen wird, welches den grenzüberschreitenden Datenverkehr erleichtert und die Attraktivität der Schweiz für neue Aktivitäten im Zusammenhang mit der digitalen Gesellschaft steigert (Ziff. 1.3 des Erläuterungsberichts). Diesen Zielsetzungen, das heisst der Förderung der Wettbewerbsfähigkeit, der Gewährleistung des freien Verkehrs personenbezogener Daten und der Chancennutzung im Bereich der Digitalisierung, wird der Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes nicht gerecht. Exemplarisch zeigt sich dies bereits in der Zweckbestimmung: Gemäss Art. 1 VE-DSG wird einseitig lediglich der Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen bezweckt. Die Stärkung der Wettbewerbsfähigkeit der Schweiz oder die Erleichterung des freien Verkehrs personenbezogener Daten wird dagegen nicht verankert. Damit missachtet der Vorentwurf, dass das Recht auf Schutz der personenbezogenen Daten kein absolutes bzw. uneingeschränktes Recht ist, sondern dass es unter Wahrung des Verhältnismässigkeitsprinzips gegen andere Grundrechte abgewogen werden muss.

Ebenso findet die vom Bundesrat am 20. April 2016 verabschiedete Strategie "Digitale Schweiz", mit welcher die Schweiz die Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen will, im Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes keinen genügenden Niederschlag. So sehen viele der neue Bestimmungen im VE-DSG zusätzliche Hürden und Erschwernisse vor, welche die Chancennutzung im Bereich der Digitalisierung erschweren anstatt sie zu fördern.

Die KARTAC beantragt daher, den Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes so zu überarbeiten, dass er auch den legitimen Interessen nach Erhaltung und Steigerung der Wettbewerbsfähigkeit der Schweizer Wirtschaft sowie der Chancennutzung im Bereich der Digitalisierung gerecht wird.

1.4 Abkürzung von Rechtserlassen

- DSGVO: Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Schengen-RL: Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
- SEV 108: Revisionsvorlage des Europarats-Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Stand: September 2016)
- VE-DSG: Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes vom 21. Dezember 2016

2. Ausführungen zu einzelnen Themen / Kritikpunkte und Anträge der KARTAC

Nachstehend finden sich zu ausgewählten Themenkreisen bzw. den zugehörigen Bestimmungen des VE-DSG die Überlegungen und Anträge der SPA:

2.1 Zweckbestimmung (Art. 1 VE-DSG)

- Antrag: Ergänzung des Zweckartikels (Art. 1 VE-DSG)

  Wie bereits oben unter Ziffer 1.3 dargelegt, beinhaltet der Zweckartikel einseitig nur den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, nicht aber die Förderung der Wettbewerbsfähigkeit der Schweiz, die Chancennutzung im Bereich der Digitalisierung und die Gewährleistung des freien Verkehrs personenbezogener Daten. Wir beantragen daher, den Zweckartikel wie folgt zu ergänzen (Ergänzung = unterstrichen):

  „Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden, sowie die Stärkung der Wettbewerbsfähigkeit der Schweiz und die Förderung des freien Verkehrs von Personendaten."

2.2 Grundsätze (Art. 4 VE-DSG)

- Antrag: Verzicht auf das Adjektiv „klar" in Art. 4 Abs. 3 VE-DSG

  Auf das Zusatzerfordernis, dass der Zweck „klar" erkennbar sein muss ist zu verzichten. Diese Anforderung führt zu keinem Mehrwert und würde lediglich zu unnötigen Auslegungsfragen führen. Zudem kennen weder DSGVO noch SEV 108 das Erfordernis, dass der Zweck *klar* erkennbar sein muss.

Wir beantragen daher, in Art. Abs. 3 VE-DSG das Adjektiv „klar" zu streichen:

„Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist."

- Antrag: Vermerk in der Botschaft, dass Einwilligung im Datenschutzgesetz eine gewöhnliche Willenserklärung im Sinne des Obligationenrechts ist (Art. 4 Abs. 6 VE-DSG)

  In der Botschaft zu einem neuen Datenschutzgesetz ist festzuhalten, dass es sich bei der Einwilligung im Datenschutzgesetz um eine gewöhnliche Willenserklärung im Sinne des Obligationenrechts handelt. Demnach kann Stillschweigen als affirmatives Verhalten dann genügen, wenn die Parteien dies vorab gültig vereinbart haben (Art. 6 OR).

  Diese Klarstellung dient dazu, die vom Datenschutzrecht vorgesehenen Einwilligungen in der Praxis angemessen handhaben zu können.

Vermerk in die Botschaft zum Datenschutzgesetz aufnehmen, dass die Einwilligung im Datenschutzgesetz eine gewöhnliche Willenserklärung im Sinne des Obligationenrechts ist.

2.3 Bekanntgabe ins Ausland (insbesondere Art. 5f. VE DSG)

- Antrag: Streichung von Art. 5 Abs. 1 VE-DSG

  Aus unserer Sicht hat die Aussage von Absatz 1 keine selbständige Bedeutung, soweit die in den nachfolgenden Absätzen getroffenen Regelungen eingehalten werden. Demzufolge beantragen wir, Absatz 1 von Artikel 5 VE-DSG ersatzlos zu streichen.

Streichung von Art. 5 Abs. 1 VE-DSG

- Antrag: Ergänzung von Art. 5 Abs. 3 VE-DSG

  Für den Fall, dass (noch) kein Entscheid des Bundesrats hinsichtlich der Angemessenheit des Datenschutzes in einem Land vorliegt, soll aus Gründen der Praktikabilität und zur Vermeidung von unnötigen Verzögerungen weiterhin der Verantwortliche die Angemessenheit eigenverantwortlich prüfen können. Entsprechend beantragen wir Art. 5 Abs. 3 VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

„Liegt kein Entscheid des Bundesrats nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist, oder wenn ein geeigneter Schutz gewährleistet ist durch: [...]

- Antrag: Streichung der in Art. 5 Abs. 3 lit. c. Ziff. 1 und lit. d. sowie in Abs. 5 VE-DSG postulierten Genehmigungspflichten

  Die in Art. 5 Abs. 3 lit. c. Ziff. 1 und lit. d. sowie in Abs. 5 VE-DSG vorausgesetzten Genehmigungen durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragten) führen zu weit. Solche Pflichten würden zu erheblichen Mehraufwänden und zu Projektverzögerungen bei den betroffenen Unternehmen führen – nicht zuletzt auch deshalb, weil sie die Kapazitäten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragten) überbeanspruchen würden und so keine angemessenen Genehmigungsfristen gegeben wären (auch wenn Ordnungsfristen ins Gesetz

aufgenommen würden). Zudem würde eine Genehmigungspflicht nicht zu einem besseren Datenschutz beitragen, steht doch das Unternehmen ohnehin selbst in der Verantwortung. Folgerichtig sieht die DSGVO keine solchen Genehmigungspflichten vor. Die vom VE-DSG vorgesehenen Genehmigungspflichten wären ein überschiessender Swiss Finish, welcher den grenzüberschreitenden Datenfluss erheblich und ohne Nutzen erschweren würde. Entsprechend beantragen wir, in Art. 5 in Abs. 3 lit. c. Ziff. 1 und lit. d. sowie in Abs. 5 VE-DSG folgende Streichungen vorzunehmen:

„Liegt kein Entscheid des Bundesrats nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist, oder wenn ein geeigneter Schutz gewährleistet ist durch:
[...]
c. standardisierte Garantien, insbesondere durch Vertrag;
~~1. welche der Beauftragte vorgängig genehmigt hat, oder~~
2. welche der Beauftragte ausgestellt oder anerkannt hat;
d. verbindliche unternehmensinterne Datenschutzvorschriften;~~, die vorgängig genehmigt wurden:~~
~~1. durch den Beauftragten, oder~~
~~2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet~~.
[...]
~~Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.~~"

- Antrag: Streichung von Art. 5 Abs. 6 VE-DSG

  In Art. 5 Abs. 6 VE-DSG soll eine Meldepflicht angeordnet werden. Dies ist unseres Erachtens systemfremd, geht es doch um bereits vorliegende, standardisierte Garantien. Weshalb die Verwendung solcher Standards in jedem Verwendungsfall erneut eine Meldepflicht auslösen sollen, ist für uns nicht nachvollziehbar. Dies umso weniger, als es sich auch dabei gegenüber dem EU-Recht um einen Swiss Finish handelt (vgl. EuGH-Entscheid Schrems und gestützt darauf ergangener Entscheid der EU-Kommission vom 16.12.2016, wonach von ihr genehmigte Datenschutz-Standardklauseln nicht einer erneuten Bewilligung im Einzelfall bedürfen und deshalb ohne Einschränkung verwendet werden dürfen; Art. 46 DSGVO). Demzufolge beantragen wir, Absatz 6 von Artikel 5 VE-DSG ersatzlos zu streichen.

  Streichung von Art. 5 Abs. 6 VE-DSG

- Antrag: Streichung von „im Einzelfall" in Art. 6 Abs. 1 lit. a. VE-DSG

  Die Einschränkung „im Einzelfall" ist nicht notwendig und nicht sinnvoll. Auch im Falle wiederholter Sachverhalte reicht bei Erkennbarkeit und entsprechendem Erwartungshorizont eine einmalige Einwilligung aus. Der Zusatz „im Einzelfall" widerspricht zudem der Gesetzessystematik, weil nur für die in Art. 6 Abs. 1 unter lit. c. und d genannten Fälle die „Bekanntgabe im Einzelfall" geregelt wird. Entsprechend beantragen wir, in Art. 6 Abs. 1 lit. a. VE-DSG folgende Streichungen vorzunehmen:

„In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:
a. die betroffene Person ~~im Einzelfall~~ eingewilligt hat;
[...]"

- Antrag: Erweiterung der Zulässigkeit der Datenübermittlung im Zusammenhang mit Verträgen in Art. 6 Abs. 1 lit. b. VE-DSG

  Ganz grundsätzlich, aber auch im Vergleich zur europäischen Lösung, ist der vorgeschlagene Art. 6 Abs. 1 lit. b. VE-DSG zu eng gefasst. Im Zusammenhang mit Verträgen sollen nicht nur die Daten des jeweiligen Vertragspartners sondern insbesondere auch Daten, welche zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags nötig sind, übermittelt werden können (vgl. auch Art. 49 Abs. 1 lit. c. DSGVO). Wir beantragen, Art. 6 Abs. 1 lit. b. VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

„In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:
a. [...]
b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners oder von Personen, in deren Interesse der Vertrag abgeschlossen werden soll, handelt;
[...]"

- Antrag: Ergänzung von in Art. 6 Abs. 1 lit. c. Ziff. 1 VE-DSG um den Fall der Übermittlung von Personendaten aus eigenem überwiegenden Interesse

  Im VE-DSG fehlt (weiterhin) eine Bestimmung, welche eine Übermittlung von Personendaten „aus eigenem überwiegenden Interesse" ermöglicht, wie dies Art. 12 Abs. 4 lit. c. SEV 108 und Art. 49 Abs. 1 DSGVO vorsehen. Wir beantragen daher, Art. 6 Abs. 1 lit. c. Ziff. 1 VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

„In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:
[...]
c. die Bekanntgabe im Einzelfall unerlässlich ist für:
1. die Wahrung eines überwiegenden öffentlichen oder privaten Interesses, oder
[...]"

- Antrag: Einengung der Meldepflicht in Art. 6 Abs. 2 VE-DSG

  Die Mitteilung an den Beauftragten, wenn Personendaten zur Vertragsabwicklung oder zur Durchsetzung von Rechtsansprüchen übermittelt werden, ist unverhältnismässig und ohne Nutzen. Es ist deshalb darauf zu verzichten.

  Wir beantragen, in Art. 6 Abs. 2 VE-DSG folgende Anpassungen (= unterstrichen) vorzunehmen:

„Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b (nur bei Abschluss eines Vertrags), c Ziffer 1 und d bekannt gibt."

2.4 Auftragsdatenbearbeitung (insbesondere Art. 7 VE DSG)

- Antrag: Keine zusätzlichen Präzisierungen der Pflichten des Auftragsbearbeiters durch den Bundesrat (Art. 7 Abs. 2 VE-DSG)

  In Art. 7 Abs. 2 VE-DSG soll der Bundesrat verpflichtet werden, die weiteren Pflichten des Auftragsbearbeiters zu präzisieren. Dafür bestehen – neben den gesetzlichen Regeln und den vertraglichen Vereinbarungen zwischen Verantwortlichem und Auftragsbearbeiter – keine Notwendigkeit und kein Bedarf. Zudem könnte – falls es wider Erwarten doch noch einen zusätzlichen Regelungsbedarf gäbe – auf die Empfehlungen der guten Praxis des Beauftragten abgestützt werden, womit das Thema an der fachlich kompetentesten staatlichen Stelle verortet wäre. Wir beantragen daher, in Art. 7 Abs. 2 VE-DSG folgende Streichung vorzunehmen:

  „Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. ~~Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.~~"

- Antrag: Präzisierung des Begriffs „anderer Auftragsbearbeiter" in Art. 7 Abs. 3 VE-DSG

  Es besteht unseres Erachtens Unklarheit darüber, wer als „anderer Auftragsbearbeiter" im Sinne von Art. 7 Abs. 3 DSG gilt. Der Terminus sollte begrifflich eng gefasst werden, damit – nebst jedwedem Unterbeauftragten – potenziell nicht auch jedwede Verhältnisse zu Hilfspersonen erfasst werden (beispielsweise im Rahmen von IT-Leistungen, bei denen zwar grundsätzlich Kontakt zu Personendaten besteht, die Leistung des Dritten jedoch nicht die Bearbeitung der Daten selbst vorsieht). Wir beantragen daher, in Art. 7 Abs. 3 VE-DSG folgende Anpassung (= unterstrichen) vorzunehmen:

  „Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem ~~anderen Auftragsbearbeiter~~ Unterbeauftragten übertragen."

- Antrag: Zustimmung soll in Form einer allgemeinen schriftlichen Einwilligung erteilt werden können (Art. 7 Abs. 3 VE-DSG)

  Die in Art. 7 Abs. 3 VE-DSG postulierte stetige vorgängige schriftliche Zustimmung des Verantwortlichen gegenüber dem Auftragsbearbeiter bei Übertragung der Bearbeitung an einen anderen Auftragsbearbeiter ist zu umständlich und daher nicht praxistauglich. Sie bringt auch keinen Nutzen für die betroffene Person. Zudem stellt sie gegenüber dem europäischen Referenzrahmen einen unnötigen Swiss Finish dar. Die europäische Regelung sieht vor, dass der vom Verantwortlichen beauftragte Auftragsverarbeiter auch auf Basis einer allgemeinen schriftlichen Einwilligung weitere Auftragsverarbeiter in Anspruch nehmen kann, wenn er den Verantwortlichen hierüber informiert, wodurch der Verantwortliche die Möglichkeit erhält hiergegen Einspruch zu erheben. Im Erläuternden Bericht zum Vorentwurf wird zwar unter Ziff. 8.1.2.4 die Zulässigkeit einer allgemeinen Einverständniserklärung erwähnt, jedoch sollte sich dies aus Gründen der Rechtssicherheit explizit so aus dem Gesetz ergeben. Wir beantragen daher, Art. 7 Abs. 3 VE-DSG wie folgt zu ergänzen (Anpassung bzw. Ergänzung = unterstrichen):

  „Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem ~~anderen Auftragsbearbeiter~~ Unterbeauftragten übertragen. Diese Zustimmung kann in genereller Weise erteilt werden."

- Antrag: Seriöse Abstimmung zwischen Datenschutzgesetz und Aufsichtspraxis der FINMA (FINMA-Rundschreiben)

  Für Finanzintermediäre bestehen mit dem sich derzeit in Überarbeitung befindlichen FINMA-Rundschreiben 2008/7 (Outsourcing Banken) und mit Anhang 3 zum FINMA-Rundschreiben 2008/21 (Operationelle Risiken Banken) bereits weitreichende Vorgaben zum Outsourcing und zum Umgang mit elektronischen Kundendaten. Diese Vorgaben dürfen durch die Neufassung des Datenschutzgesetzes nicht weiter verschärft werden, und es darf auch nicht zu Redundanzen oder Widersprüchen in der praktischen Umsetzung der verschiedenen Vorgaben kommen.

  Das neue Datenschutzgesetz ist mit der Aufsichtspraxis der FINMA (FINMA-RS) im Bereich Outsourcing/Umgang mit elektronischen Kundendaten abzustimmen.

2.5 Profiling (insbesondere Art. 3 lit. f., Art. 4 Abs. 6, Art. 23 Abs. 2 lit. d., Art. 24 Abs. 2 VE-DSG)

- Antrag: Die Begriffsbestimmung „Profiling" in Art. 3 lit. f. VE-DSG ist enger zu fassen: Kein Einbezug von Nicht-Personendaten und kein Einbezug nicht-automatisierter Datenbearbeitung

  Die in Art. 3 lit. f. VE-DSG vorgesehene Regelung umfasst im Gegensatz zur Regelung der DSGVO (Art. 4 Ziff. 4) auch die Verarbeitung nicht-personenbezogener Daten sowie die nicht-automatisierte Auswertung von Daten. Zudem schränkt der Wortlaut der Bestimmung den Anwendungsbereich nicht auf das Profiling der Daten einer bestimmten betroffenen Person ein. Der Wortlaut umfasst somit auch eine Auswertung von anonymen Daten und potenziell auch eine Auswertung hinsichtlich der Merkmale von Personengruppen. Damit geht der Vorentwurf nicht nur ganz erheblich über die Regelung auf europäischer Ebene hinaus (Swiss Finish), sondern schiesst ganz generell über das Ziel hinaus. Die vorgeschlagene weite Begriffsbestimmung des Profiling würde zu einschneidenden Einschränkungen und neuen Risiken in der Datenbearbeitung für Unternehmen führen – und das ganz besonders auch in Bezug auf statistische Auswertungen und Forschungstätigkeiten. Viele Datenbearbeitungen zu statistischen Zwecken oder bei der Entwicklung neuer Produkte und Leistungen werden mit Daten vorgenommen, die nicht personenbezogen sind. Eine solche Datenbearbeitung stellt für die Persönlichkeit der betroffenen Person kein erhöhtes Risiko dar, da die Auswertung anonymisiert erfolgt, weshalb eine Subsumierung solcher Tätigkeiten unter den Begriff „Profiling" unangebracht bzw. unverhältnismässig wäre.

  Dasselbe gilt für den Fall, dass Daten nicht automatisiert ausgewertet werden. In solchen Fällen kann sich kein erhöhtes Risiko für die betroffene Person ergeben, da keine aus der Datenauswertung resultierenden automatisierten Entscheidungen erfolgen. Nicht-automatisiertes Profiling unterliegt zudem als Datenbearbeitung ganz normal dem Datenschutzgesetz. Den Schutz darüber hinaus durch die Ausweitung des Begriffs „Profiling" weiter zu erhöhen, entbehrt einer Grundlage und lässt sich daher nicht rechtfertigen.

  Wir beantragen, die Begriffsbestimmung zum Profiling enger zu fassen und auf den Einbezug von Nicht-Personendaten und von nicht-automatisierter Datenbearbeitung zu verzichten. Zudem ist klarzustellen, dass sich Profiling immer auf eine bestimmte Person beziehen muss und nicht die Auswertung hinsichtlich ganzer Personengruppen oder

Segmente umfasst. Wir beantragen daher, in Art. 3 lit. f. VE-DSG folgende Anpassungen (= unterstrichen) vorzunehmen:

„Profiling: jede automatisierte Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale der betroffenen Person zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich ihrer Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, Intimsphäre oder Mobilität."

- Antrag: Keine *ausdrückliche* Einwilligung für das Profiling (Art. 4 Abs. 6 VE-DSG)

  Weder DSGVO noch SEV 108 verlangen generell die Ausdrücklichkeit der Einwilligung in das Profiling. Der VE-DSG will in Art. 4 Abs. 6 darüber hinausgehen und generell eine *ausdrückliche* Einwilligung für das Profiling statuieren. Auf diesen Swiss Finish ist zu verzichten. Wir beantragen, dass auf die generelle Anforderung, dass eine Einwilligung ins Profiling immer ausdrücklich erfolgen muss, zu verzichten und folgende Streichung in Art. 4 Abs. 6 VE-DSG vorzunehmen ist:

  „Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen."

- Antrag: Profiling ohne *ausdrückliche* Einwilligung stellt keine Persönlichkeitsverletzung dar (Art. 23 Abs. 2 lit. d. VE-DSG)

  In Konsequenz der vorstehenden Erörterungen ist es auch nicht angemessen, ein Profiling ohne *ausdrückliche* Einwilligung als Persönlichkeitsverletzung zu taxieren.

  Wir beantragen daher, Buchstabe d. von Art. 23 Abs. 2 VE-DSG ersatzlos zu streichen.

  „Eine Persönlichkeitsverletzung liegt insbesondere vor:
  [...]
  ~~d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.~~

- Antrag: Verankerung eines Rechtfertigungstatbestandes für das Profiling (Art 24 Abs. 2 VE-DSG)

  23 Abs. 2 lit. d. VE-DSG legt zudem nahe, dass eine Rechtfertigung des Profilings ausschliesslich über eine ausdrückliche Einwilligung möglich ist und somit Profiling nie nach Art. 24 VE-DSG gerechtfertigt sein kann. Das führt zu weit und würde sich insbesondere für die Anbieter von Zahlungsdienstleistungen verheerend auswirken. Für Zahlungsdienstanbieter sind Datenbearbeitungen, inklusive Profiling, insbesondere zur Bekämpfung von Betrug, zur Vermeidung von Kreditausfällen und zur Erhöhung der Sicherheit unverzichtbar – und das gleichermassen im Interesse der Konsumentinnen/Konsumenten und Händler, welche die Zahlungsmittel nutzen, wie der Zahlungsdienstleister selbst. Dabei müssen die Datenbearbeitungen bzw. die Profile regelmässig den neuesten Bedrohungen und den eingetretenen Veränderungen angepasst und entsprechend weiterentwickelt werden können. Eine Rechtfertigung dieser Datenbearbeitungen muss daher weiterhin ohne ausdrückliche Einwilligung und gestützt auf ein überwiegendes Interesse zulässig sein. Alles andere wäre unpraktikabel und würde die effiziente und effektive Betrugsbekämpfung und Vorbeugung von Kreditausfällen unnötig beeinträchtigen.

  Wir beantragen daher, in Art. 24 Abs. 2 VE-DSG einen weiteren Rechtfertigungstatbestand einzuführen bzw. Art 24 Abs. 2 VE-DSG wie folgt zu ergänzen (lit. g.):

„Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere:
[...]
g. die Daten zur Erhöhung der Sicherheit und Vermeidung von erheblichen Nachteilen für die betroffenen Personen bearbeitet, wofür sie auch Profiling betreiben kann.

2.6 Informationspflichten gegenüber der betroffenen Person (insbesondere Art. 13, 14 und 15 VE-DSG)

- Antrag: Streichung von Art. 13 Abs. 4 VE-DSG

  Gemäss der der in Art. 13 Abs. 4 VE-DSG vorgeschlagenen Bestimmung hat der Verantwortliche die betroffene Person über die Identität und die Kontaktdaten der Auftragsbearbeiter – und konsequenterweise auch aller Unterauftragsbearbeiter – zu informieren. Dies geht sowohl über die DSGVO als auch die SEV 108 hinaus und wäre in der Praxis unverhältnismässig aufwändig bzw. würde die Geschäftsprozesse ungerechtfertigt behindern. Faktisch würde eine sinnvolle Auftragsdatenbearbeitung verunmöglicht. Eine solche Bestimmung ist aber auch deshalb nicht nötig, weil die Auslagerung von Dienstleistungen und der zugehörigen Datenbearbeitungen zum täglichen Geschäftsbetrieb jedes Unternehmens gehört und die betroffene Person weiss bzw. davon ausgeht, dass nicht jedes Unternehmen sämtliche Dienstleistungen selbst erbringen kann bzw. erbringt. Aus Sicht des Persönlichkeitsschutzes ist nicht entscheidend, dass die betroffene Person Identität und Kontaktdaten des Auftragsbearbeiters kennt, sondern dass sichergestellt ist, dass die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben erfolgt. Dies zu regeln ist Gegenstand von Art. 7 VE-DSG. Eine darüberhinausgehende Informationspflicht bringt aus datenschutzrechtlicher Sicht keinerlei Mehrwert, verursacht jedoch gewichtige Nachteile.

  Ergänzend ist darauf hinzuweisen, dass generell die rechtsgenügliche Möglichkeit bestehen muss, dass bei der Beschaffung von Personendaten auf eine bestimmte Plattform (z.B. Webseite) verwiesen werden kann, wo detaillierte Informationen zur Datenbearbeitung eingesehen werden können. Dies würde die Vorgaben der SEV 108 erfüllen, wonach der Zugang zu den Informationen gesichert sein muss. Die Erläuterungen zum VE-DSG lassen demgegenüber vermuten, dass es nach dem aktuellen Vorentwurf nicht ausreicht, wenn die betroffene Person bereitgestellte Informationen selbst abrufen bzw. konsultieren muss.

  Wir beantragen, Art. 13 Abs. 4 VE-DSG zu streichen.

  Streichung von Art. 13 Abs. 4 VE-DSG.

- Antrag: Streichung von Art. 13 Abs. 5 VE-DSG

  Für den Verantwortlichen ist es zur Wahrung seiner berechtigten Interessen erforderlich, dass Personendaten auch aus Drittquellen (z.B. Wirtschaftsauskunfteien oder Marketingdatenbanken) bezogen werden können, um z.B. Kreditprüfungen oder die Allokation von Werbemitteln effektiv, fokussiert und effizient durchführen zu können. Eine generelle Information der betroffenen Person über die Möglichkeit eines Bezuges von Personendaten aus Drittquellen ist bei einer Geschäftsanbahnung zwischen dem Verantwortlichen und der betroffenen Person ggf. noch gangbar (z.B. durch Hinweis in den AGB). Sollte eine explizite Information unmittelbar im Zeitpunkt der Informationsbeschaffung bei Drit-

ten vorgesehen und gemeint sein, so ist dies nicht praktizier- und umsetzbar. Im Besonderen dürften Wirtschaftsauskunfteien und Marketingdatenbanken, die Personendaten aus Drittquellen beziehen und verarbeiten, durch die vorgesehenen Regelungen in Art. 13 Abs. 5 nachhaltig beeinträchtigt werden, da sie nicht in einer unmittelbaren Geschäftsbeziehung zur betroffenen Person stehen. Im Ergebnis müsste für Kreditentscheide und Marketing-Massnahmen auf entscheidungsrelevante Informationen verzichtet werden, die erhöhte Kreditausfälle und breite, ineffiziente Streuung von Werbemitteln und Angeboten zur Folge haben können. Zur Wahrung der berechtigten Interessen der Verantwortlichen beantragen wir daher Art. 13 Abs. 5 VE-DSG ersatzlos zu streichen.

Streichung von Art. 13 Abs. 5 VE-DSG.

- Antrag: Verzicht auf die in Art. 14 Abs. 4 lit. a VE-DSG enthaltene Einschränkung „und er die Personendaten nicht Dritten bekannt gibt"

  Für die in Art. 14 Abs. 4 lit. a VE-DSG formulierte Einschränkung „und er die Personendaten nicht Dritten bekannt gibt" gibt es aus datenschutzrechtlichen Überlegungen keinerlei Berechtigung: Sollten die Interessen der betroffenen Person durch die Bekanntgabe an einen Dritten tatsächlich beeinträchtigt sein, so ist dies bereits im Rahmen der allgemeinen Interessenabwägung im Sinne von Art. 24 VE-DSG berücksichtigt. Alles andere wäre das Resultat einer pauschal vorweggenommenen Interessenabwägung und würde zu absurden Situationen führen: So dürfte ein Konzernunternehmen, welches Daten mit einem anderen Konzernunternehmen teilt, nicht auf ein überwiegendes eigenes Interesse abstellen, während ein Unternehmen, das Daten innerhalb der gleichen juristischen Person ins Ausland liefert, dies nach wie vor könnte.

  Wir beantragen daher, Art. 14 Abs. 4 lit. a wie folgt anzupassen:

  „Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten:

  a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt~~;"

- Antrag: Streichung von Art. 14 Abs. 5 VE-DSG

  Die in Art 14 Abs. 5 statuierte Pflicht, beim Wegfall des Grundes für den Verzicht, die Einschränkung oder das Aufschieben die Information nachträglich mitzuteilen, ist ohne grossen Nutzen, würde aber unverhältnismässig hohen Aufwand verursachen. Eine solche Pflicht hätte zur Folge, dass Unternehmen über jede einzelne, gestützt auf eine Interessenabwägung gefällte Entscheidung für einen Informationsverzicht etc. Buch führen müssten, um diese Entscheidungen anschliessend permanent zu überwachen und sicherzustellen, dass – wenn beispielsweise keine überwiegenden Interessen Dritter mehr vorliegen – die nun fällige werdende Information nachgeholt würde. Das ist vollkommen unpraktikabel.

  Wir beantragen daher, Art. 14 Abs. 5 VE-DSG ersatzlos zu streichen.

  Streichung von Art. 14 Abs. 5 VE-DSG.

- Antrag: Präzisierung und Anpassung von Art. 15 Abs. 1 VE-DSG

  Die in Art. 15 Abs. 1 dargelegte Informationspflicht bei einer automatisierten Einzelentscheidung lässt offen zu welchem Zeitpunkt die betroffene Person zu informieren ist und

ob diese Information jeweils explizit im Zeitpunkt der einzelnen Entscheidung zu erfolgen hat. Eine explizite Information im Zeitpunkt der Einzelentscheidung ist in vielen Fällen nicht praktizier- und umsetzbar (z.B. Entscheidungen über die Bereitstellung eines Zahlungsmittels im Bezahlprozess im E-Commerce). Die Information über automatisierte Einzelentscheidungen muss daher generell (z.B. durch die Bekanntgabe in den AGB) erfolgen können

Wir beantragen daher, Art. 15 Abs. 1 VE-DSG wie folgt anzupassen.

Der Verantwortliche informiert die betroffene Person darüber, ~~wenn eine Entscheidung erfolgt~~ dass er Entscheidungen trifft, die ausschliesslich auf einer automatisierten Datenbearbeitung beruhen ~~beruht~~, ~~und~~ sofern diese Entscheidungen rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person haben ~~hat~~.

- Antrag: Streichung des in Art. 15 Abs. 2 VE-DSG vorgesehene Äusserungsrechts zu den bearbeiteten Personendaten

  Eine Datenbearbeitung mit ausschliesslich automatisierten Mitteln ist per se kein schwererer Eingriff in Persönlichkeitsrechte als eine rein "menschliche" Bearbeitung. Im Gegenteil, eine algorithmenbasierte Datenbearbeitung, die den zwingenden Grundsätzen der Privacy by Default und Design folgt, bietet eine grössere Gewähr der Rechtskonformität; der Risikofaktor "Mensch" kann hier ausgeschlossen werden. Aus diesem Grund ist das fragliche Äusserungsrecht für die betroffene Person unverhältnismässig und ein sachlich nicht begründeter Ausdruck eines generellen Misstrauens gegenüber "der Maschine".

  Wir beantragen daher, Art. 15 Abs. 2 VE-DSG ersatzlos zu streichen.

Streichung von Art. 15 Abs. 2 VE-DSG.

- Antrag: Verzicht auf die in Art. 15 Abs. 3 VE-DSG vorgesehene Informationspflicht gestützt auf eine Vereinbarung zwischen der betroffenen Person und dem Verantwortlichen

  Die Informationspflicht betreffend automatisierte Einzelentscheidungen sollte nicht nur wegfallen, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht, sondern auch dann, wenn die automatisierten Einzelentscheidungen gestützt auf eine Vereinbarung zwischen der betroffenen Person und dem Verantwortlichen gefällt werden und sie den erkennbaren Kern der Vereinbarung ausmachen. Dies kann z.B. bei einem Vertrag betreffend die automatisierte Verwaltung des Vermögens der betroffenen Person gegeben sein (z.B. RoboAdvice – hier möchte der Kunde gerade ausschliesslich automatisierte Einzelentscheidungen). In solchen Fällen sind der betroffenen Person die zugrundeliegenden Parameter bekannt bzw. sie hat diese mit dem Verantwortlichen vereinbart. Entsprechend beantragen wir, dass in Art. 15 Abs. 3 VE-DSG festgehalten wird, dass die Informationspflicht nicht besteht, wenn eine Vereinbarung zwischen dem Verantwortlichen und der betroffenen Person die Abgabe (ev. einer Vielzahl) von automatisierten Einzelentscheidungen bezweckt und dies aus der Vereinbarung erkennbar ist. Dies umso mehr, als eine Schlechterstellung einer erkennbaren Datenbearbeitung im privaten Bereich gegenüber dem öffentlich-rechtlichen (Gesetz) nicht gerechtfertigt ist.

  Wir beantragen daher, Art. 15 Abs. 3 VE-DSG wie folgt zu ergänzen (Ergänzungen = unterstrichen):

Die Informations~~- und Anhörungs~~pflicht gilt nicht, wenn ein Gesetz oder ein Vertrag zwischen Verantwortlichem und betroffener Person eine automatisierte Einzelentscheidung ~~vorsieht~~ vorsehen.

2.7 Datenschutz-Folgenabschätzung (Art. 16 VE-DSG)

- Antrag: Streichung von Art. 16 VE-DSG

  Zur Einhaltung der Bestimmungen des Datenschutzgesetzes braucht ein Unternehmen bereits heute laufend fachkundige Beurteilungen und darauf abgestützte Massnahmenpakete. Diese Grundvoraussetzung – speziell das Durchführen einer Datenschutz-Folgenabschätzung (DFA) – gesetzlich zu verankern, bringt keinen Mehrwert, sondern verursacht – insbesondere auch in Zusammenhang mit der Konsultationspflicht beim Beauftragten – erhebliche Rechtsunsicherheit und das Risiko von ungerechtfertigten Verzögerungen.

  Wir beantragen daher, Art. 16 VE-DSG ersatzlos zu streichen.

  Streichung von Art. 16 VE-DSG.

  - Eventualantrag 1: Präzisierung von Art. 16 VE-DSG

    Sollte entgegen dem vorstehenden Antrag an Art. 16 VE-DSG grundsätzlich festgehalten werden, beantragen wir, die unglückliche Formulierung von Absatz 1 („... voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person, ...") anzupassen.

    Einerseits beantragen wir „erhöht" durch „hoch" zu ersetzen, um klarzustellen, welcher Risikograd gemeint ist (vgl. auch Art. 35 Abs. 1 und Erwägung 91 DSGVO). Eine gesetzliche Pflicht zur Datenschutz-Folgenabschätzung soll auf Datenbearbeitungen mit hohen Risiken beschränkt werden. Damit sind nach EU-Doktrin solche gemeint, welche auch nach Implementierung geeigneter Massnahmen immer noch hohe Risiken aufweisen. Andernfalls würde dies – da jede Datenbearbeitung zu einem erhöhten Risiko gegenüber keiner Bearbeitung führt – bedeuten, dass letztlich bei jeder Datenbearbeitung eine formelle DFA durchzuführen wäre. Dies hätte zur Folge, dass neue Vorhaben, für die Personendaten bearbeitet werden müssen, stark verzögert würden. Nicht zu unterschätzen wären auch der Mehraufwand und die Notwendigkeit von zusätzlichen Ressourcen für das Management von DFA. Insbesondere für kleinere Unternehmen oder Startups würde dies prohibitiv wirken.

    Andererseits beantragen wir, die Begriffe „Persönlichkeit oder Grundrechte" durch den Begriff „Persönlichkeitsverletzung" zu ersetzen; dies entsprechend der Schweizer Gesetzesterminologie (vgl. dazu auch Art. 23 ff. VE-DSG).

    Schliesslich ist es auch unglücklich, dass in Art. 16 VE-DSG mehrmals vom „Verantwortlichen oder vom Auftragsbearbeiter" gesprochen wird. Dies führt zu einer Verwischung der Verantwortlichkeit bzw. zu Unsicherheiten, wem die jeweilige Pflicht obliegt. Wir beantragen, (durch Weglassung des Auftragsbearbeiters) klar zu stellen, dass nur der Verantwortliche die Verantwortung für Durchführung einer DFA trägt.

    Damit beantragen wir eventualiter Art. 16 VE-DSG wie folgt anzupassen (Anpassungen = unterstrichen):

„Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem ~~erhöhten~~ hohen Risiko ~~für die Persönlichkeit oder die Grundrechte~~ einer Persönlichkeitsverletzung der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.

Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer ~~Verletzung der Persönlichkeit oder der Grundrechte~~ Persönlichkeitsverletzung der betroffenen Person zu verringern.

Der Verantwortliche ~~oder der Auftragsbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen.

Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von drei Monat nach Erhalt aller erforderlichen Informationen mit."

- Eventualantrag 2: Streichung von Art. 16 Abs. 3 und 4 VE-DSG

  Sollte entgegen dem obenstehenden Antrag an Art. 16 VE-DSG grundsätzlich festgehalten werden, beantragen wir, zumindest die Absätze 3 und 4 zu streichen. Die Konsultationspflicht beim Beauftragten schiesst über das Ziel – und auch über das europäische Regulierungsniveau – hinaus. Gemäss DSGVO ist eine Konsultation nur bei erheblichen Restrisiken vorgesehen (vgl. Art. 36 DSGVO und Erwägung 84). Darüber hinaus ist die vorgesehene dreimonatige Frist für Einwände des Beauftragten zu lange und schafft auch keinerlei Mehrwert, da weder eine Sperrwirkung vorgesehen ist, noch die Einwände als Präjudiz gelten sollen. Hingegen wirkt sie als Innovationshemmer und behindert die internationale Wettbewerbsfähigkeit der Schweizer Wirtschaft (unnötige Verlängerung der time to market). Dass darüber hinaus der Beauftragte später (auch falls er sich nicht vernehmen liess) noch eine Untersuchung soll einleiten können, schafft zusätzlich Rechtsunsicherheit. Schliesslich würde durch die vorgesehene Konsultationspflicht auch beim Beauftragten ein erheblicher Bürokratieschub bzw. ein erheblicher Mehraufwand entstehen, was sich insgesamt nachteilig auf die Zusammenarbeit zwischen Wirtschaft und Beauftragtem bzw. nachteilig auf die Wettbewerbsfähigkeit der Schweizer Wirtschaft auswirken dürfte.

  Damit beantragen wir eventualiter, Art. 16 Abs. 3 und 4 VE-DSG ersatzlos zu streichen.

Streichung von Art. 16 Abs. 3 und 4 VE-DSG.

2.8 Meldungen von Verletzungen des Datenschutzes (Art. 17 VE-DSG)

- Antrag: Präzisierungen und Ergänzungen von Art. 17 VE-DSG

  Die in Absatz 1 und 4 von Art. 17 VE-DSG enthaltene Formulierung, dass Meldungen „unverzüglich" zu erfolgen haben, ist zu absolut (auch gegenüber der DSGVO, welche in Art. 33 Abs. 1 als Richtschnur 72 Stunden angibt). Wir beantragen daher, dass die Meldungen „ohne unnötigen Verzug" zu erfolgen haben.

  Weiter ist in Absatz 1 von Art. 17 festgehalten, dass Meldungen bei „unbefugter Datenbearbeitung oder Verlust von Daten" zu erstatten sind. Wir erachten diese Begriffe als

unzutreffend. Schutzobjekt ist die Sicherheit von Personendaten, weshalb wir beantragen, diese Terminologie zu verwenden, womit Meldungen dann zu erfolgen haben, wenn eine Verletzung der Sicherheit von Personendaten vorliegt.

Schliesslich ist zur Gewährleistung einer hohen Praxistauglichkeit von Art. 17 auch sicherzustellen, dass die verlangten Meldungen bzw. „Selbstanzeigen" ohne strafrechtliche Konsequenzen bleiben.

Abschliessend ist in Absatz 2 von Art. 17 im Sinne einer verhältnismässigen Regelung nur dann eine Informationspflicht an die betroffene Person zu statuieren, wenn der Beauftragte diese Information verlangt. Damit ergibt sich aus der Meldung des Verantwortlichen an den Beauftragten ein konkreter Nutzen für den Verantwortlichen.

Somit beantragen wir, Art. 17 VE-DSG wie folgt anzupassen (Anpassungen = unterstrichen):

Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ ohne unnötigen Verzug eine Verletzung der Sicherheit von Personendaten ~~unbefugte Datenbearbeitung oder den Verlust von Daten~~, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person. Die gemeldete Verletzung wird strafrechtlich nicht verfolgt. Der Verantwortliche informiert ausserdem die betroffene Person, wenn ~~es zum Schutz der betroffenen Person erforderlich ist oder~~ der Beauftragte es verlangt. Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. Der Auftragsbearbeiter informiert den Verantwortlichen ~~unverzüglich~~ ohne unnötigen Verzug über eine Verletzung gemäss Absatz 1. ~~unbefugte Datenbearbeitung~~.

2.9 Weitere Pflichten des Verantwortlichen und des Auftragsbearbeiters (Art. 19 VE-DSG)

- Antrag: Reduktion bzw. engere Umschreibung der Weiteren Pflichten in Art. 19 VE-DSG

  Umfang und Inhalt der uneingeschränkten Dokumentationspflicht gemäss Art. 19 lit. a VE-DSG sind unklar. Offensichtlich ist aber, dass die vorgeschlagene Regelung über die vergleichbare Bestimmung der DSGVO (Art. 30) hinausgeht. Letztere verlangt ein Verzeichnis. Ein solches – und nur ein solches – ist auch für das Schweizer Datenschutzrecht vorzusehen. Andernfalls müsste z.B. jede E-Mail, jede Chatnachricht etc. dokumentiert werden, was mit einem unverhältnismässigen, nicht praxistauglichen Aufwand einherginge.

  Auch Art. 19 lit. b VE-DSG ist viel zu weit gefasst und unverhältnismässig. Einerseits müssten Verantwortliche und Auftragsbearbeiter über heikle bzw. sensible Datenschutzverletzungen eine Vielzahl Dritter informieren. Andererseits wäre der Aufbau einer neuen Infrastruktur, welche zentralisiert sämtliche Empfängerinnen und Empfänger von Personendaten über Jahrzehnte verwaltet im Vergleich zum Nutzen nicht verhältnismässig. Auf Art. 19 lit. b VE-DSG ist daher zu verzichten.

  Wir beantragen daher, folgende Streichungen bzw. Neuformulierung in Art. 19 VE-DSG vorzunehmen (Neuformulierung = unterstrichen):

Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet:
~~a. Sie dokumentieren ihre Datenbearbeitung~~ Sie erstellen ein Verzeichnis für regelmässige Datenbearbeitungen.
b. ~~Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2, es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.~~

2.10 Rechte der betroffenen Person (Art. 20 und 21 VE-DSG)

Kernanliegen der nachstehenden Anträge ist es, einem Missbrauch des Auskunftsrechts der betroffenen Person vorzubeugen.

- Antrag: Verzicht auf in jedem Fall kostenlose Auskunft (Art. 20 Abs. 1 VE-DSG)

  Dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke ist entgegenzuwirken. Die Praxis zeigt, dass aktuell einerseits datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln zur Vorbereitung von Gerichtsverfahren durchzusetzen. Andererseits hat die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu Schikanezwecken ebenfalls spürbar zugenommen. Damit wird das Auskunftsrecht missbräuchlich angewandt.

  Wir beantragen daher, die generelle Kostenlosigkeit der Auskunft zu streichen und stattdessen einen angemessenen Unkostenbeitrag vorzusehen. Ergänzend soll dem Bundesrat die Kompetenz eingeräumt werden, auf Verordnungsstufe festzulegen, in welchen Fällen die Auskunft kostenlos zu erteilen ist.

  Wir beantragen daher, Art. 20 Abs. 1 wie folgt anzupassen (Ergänzungen = unterstrichen):

  „Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Der Verantwortliche kann für die Auskunft einen angemessenen Unkostenbeitrag erheben. Der Bundesrat regelt, in welchen Fällen die Auskunft kostenlos erfolgt."

- Antrag: Auskunftsrecht weiterhin am System der Datensammlung anknüpfen (Art. 20 Abs. 1 VE-DSG)

  Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen sowie auch auf hängige Verfahren ist unverhältnismässig. Dies gilt umso mehr, als dass gemäss der in Schweiz geltenden Rechtsprechung kaum ein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um einen Auskunftsanspruch zu bejahen. Die fortgesetzte Anknüpfung am bisher bewährten System der Datensammlung ist sachgerecht und bietet den betroffenen Personen ausreichend Schutz.

  Wir beantragen daher, Art. 20 Abs. 1 VE-DSG (im Konnex mit unseren vorstehenden Ausführungen unter Ziffer 2.9) wie folgt zu formulieren (Ergänzung = unterstrichen):

  Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie im erstellten Verzeichnis gemäss Art. 19 bearbeitet werden.

- Antrag: Verzicht auf zu weit gefasste Informationspflichten (Art. 20 Abs. 3 VE-DSG)

  Art. 20 Abs. 3 VE-DSG ist zu weit gefasst. Zum einen ist es überschiessend, wenn bei jeder aufgrund einer Datenbearbeitung gefällten Entscheidung eine Informationspflicht bestehen würde, weshalb eine solche nur für automatisierte Einzelentscheidung vorzusehen ist. Zum anderen ist der Schluss von Art. 20 Abs. 3 VE-DSG ersatzlos zu streichen. Eine derart weitgehende Begründungs- bzw. Rechtfertigungspflicht ist ein überschiessender Swiss Finish und datenschutzrechtlich nicht zu rechtfertigen. Er würde ausserdem zwangsläufig zu einer Offenlegung von Geschäftsgeheimnissen sowie internen Entscheid- und Ablaufverfahren führen.

  Wir beantragen daher, Art. 20 Abs. 3 mittels einer Neuformulierung (= unterstrichen) und einer Streichung wie folgt anzupassen:

  > Wird aufgrund einer Datenbearbeitung eine automatisierte Einzelentscheidung gefällt, erhält die betroffene Person Informationen über das Ergebnis~~, das Zustandekommen und die Auswirkungen der Entscheidung~~.

- Antrag: Mechanismus gegen Missbrauch des Auskunftsrechts zur Prozessvorbereitung (Art. 21 VE-DSG)

  Angesichts des oben dargelegten Missbrauchs des Auskunftsrechts zur Prozessvorbereitung sollte im totalrevidierten Datenschutzgesetz ein effektiver Abwehrmechanismus vorgesehen werden. Wir schlagen diesbezüglich vor, dass der Verantwortliche die Auskunft verweigern kann, wenn das Ersuchen im Kern nicht datenschutzrechtlichen Zwecken dient. Lehnt der Verantwortliche ein Auskunftsersuchen ab, soll die betroffene Person die Möglichkeit haben zu verlangen, dass der Beauftragte entscheidet, ob das Ersuchen genügend datenschutzrechtlich motiviert ist oder nicht.

  Wir beantragen daher, den datenschutzrechtlichen Zweck als zwingende Voraussetzung für das Auskunftsrecht vorzusehen und Art. 21 um einen neuen Abs. 2 zu ergänzen (= unterstrichen):

  > „Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben.
  >
  > Ausserdem kann die Auskunft nach diesem Gesetze verweigert werden, wenn das Ersuchen im Kern nicht datenschutzrechtlichen Zwecken dient. Lehnt der Verantwortliche ein Ersuchen nach diesem Absatz ab, kann die betroffene Person verlangen, dass der Beauftragte entscheidet, ob das Ersuchen genügend datenschutzrechtlich motiviert ist.
  >
  > Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten."

  Ergänzend oder alternativ kann für den Fall eines im Kern nicht datenschutzrechtlichen Zwecken dienenden Auskunftsgesuches in Art 14 Abs. 4 VE-DSG ein zusätzlicher Rechtfertigungsgrund für die Einschränkung, Aufschiebung oder den Verzicht der Übermittlung von Informationen aufgenommen werden.

2.11 Verwaltungsrechtliche Befugnisse und strafrechtliche Sanktionen (insbesondere Art. 41ff. und Art. 50ff. VE DSG)

- Antrag: Streichung von Art. 41 Abs. 3 VE-DSG

  Dem Grundsatz „nemo tenetur" folgend, ist es unzulässig, dass dann, wenn jemand seine Mitwirkungspflicht verletzt, eine Hausdurchsuchung vorgenommen werden kann.

  Wir beantragen daher, Art. 41 Abs. 3 VE-DSG zu streichen:

Streichung von Art. 41 Abs. 3 VE-DSG

- Antrag: Streichung von Art. 44 Abs. 3 VE-DSG

  Dass Beschwerden gegen vorsorgliche Massnahmen generell keine aufschiebende Wirkung haben sollen, ist unverhältnismässig. Vorsorgliche Massnahmen können für die Betroffenen mit erheblichen Schäden bzw. Kostenfolgen verbunden sein. Es ist deshalb unerlässlich, dass sich ein Verantwortlicher gegen ein unverhältnismässiges Vorgehen in jedem Verfahrensstadium wirksam zur Wehr setzen kann.

  Wir beantragen daher, Art. 44 Abs. 3 VE-DSG zu streichen:

Streichung von Art. 44 Abs. 3 VE-DSG

- Antrag: Anzeigepflicht in Art. 45 VE-DSG in ein Anzeigerecht umwandeln

  Die in Art. 45 VE-DSG vorgesehene Anzeigepflicht stellt gegenüber dem EU-Datenschutzniveau (Anzeigerecht gemäss Art. 58 Abs. 5 DSGVO / Art. 12bis, Ziff. 2 lit. d. SEV 108) einen Swiss Finish dar, auf den zu verzichten ist.

  Wir beantragen daher, Art. 45 VE-DSG wie folgt anzupassen (Anpassungen = unterstrichen):

Art. 45 ~~Anzeigepflicht~~ Anzeigerecht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so ~~teilt~~ ist er befugt, dies den Strafverfolgungsbehörden mitzuteilen.

- Antrag: Streichung der Artikel 50 bis 55 VE-DSG

  Strafrechtliche Sanktionen sind für die Äquivalenz zum europäischen Datenschutzniveau in keiner Weise erforderlich – im Gegenteil: Sie dürften sich punkto Äquivalenz als hinderlich erweisen, da die DSGVO zur Durchsetzung das verwaltungsrechtliche Verfahren vorsieht. Darüber hinaus ist die Androhung strafrechtlicher Sanktionen – erst Recht persönlicher strafrechtlicher Sanktionen – unverhältnismässig und in hohem Masse kontraproduktiv. Ganz besonders stossend ist dabei die Strafbarkeit von fahrlässigen DSG-Verstössen. Aber auch der Bussenrahmen für Mitarbeitende von bis zu CHF 500'000 ist weit überschiessend – umso mehr als er selbst bei Fahrlässigkeit bis zu CHF 250'000 reicht. Hinzu kommt, dass viele der sanktionierten DSG-Bestimmungen – zu Recht – weniger regel- und eher prinzipienbasiert konzipiert sind. Prinzipienbasierte Normen eignen sich jedoch nicht dafür, mit strafrechtlichen Sanktionen verknüpft zu werden, da für die Rechtsunterworfenen unter strafrechtlichen Gesichtspunkten zu wenig klar bzw. zu wenig eingegrenzt ist, welches Verhalten mit Strafe bedroht ist (nulla poena sine lege stricta).

  Persönliche strafrechtliche Sanktionen würden die unternehmensinternen Entscheidungsprozesse lähmen und ein Klima schaffen, in welchem innerbetrieblich niemand

mehr bereit wäre, abschliessend Verantwortung für den Datenschutz zu übernehmen. Durch die Schaffung eines persönlichen Strafbarkeitsrisikos würde ganz besonders auch die Funktion des/der betrieblichen Datenschutzverantwortlichen untergraben (anstatt dass diese gestärkt würde). In der Konsequenz würden einerseits betriebsintern keine Entscheide mehr ohne externe Absicherung getroffen und andererseits aus Sicherheitsgründen dahingehende Selbstbeschränkung vorgenommen, dass der DSG-Rahmen nicht mehr ausgeschöpft würde. Damit wiederum würde im Datenschutz der Ausgleich zwischen den Interessen des Datenbearbeiters/des Verantwortlichen und denjenigen der betroffenen Person aus der Balance gebracht.

Wir beantragen daher die Artikel 50 bis 55 VE-DSG zu streichen und auf neue Sanktionen zu verzichten. Dies umso mehr, als die Nichteinhaltung von Verfügungen des Beauftragten bereits heute via Art. 292 StGB sanktioniert werden kann.

Verzicht auf die Art 50 bis 55 VE-DSG

Sofern das Sanktionssystem dennoch ausgebaut werden sollte, so hätte dies nach unserer Beurteilung durch die Einführung von Verwaltungsbussen zu erfolgen, die vom Beauftragten ausgesprochen werden könnten. Damit wäre zumindest erreicht, dass einerseits keine unverhältnismässigen Sanktionen gegenüber natürlichen Personen ergriffen würden und dass anderseits eine Instanz die Sanktion verhängen würde, welche mit der Materie fachlich vertraut ist (was beim kantonalen Strafrichter nicht der Fall wäre).

- Eventualanträge für den Fall, dass an strafrechtlichen Sanktionen festgehalten würde: Sollte entgegen dem vorstehenden Antrag an strafrechtlichen Sanktionen festgehalten werden, beantragen wir insbesondere folgende Anpassungen am Regime des VE-DSG:

- Überprüfung der Strafwürdigkeit einzelner Tatbestände, insbesondere der Unterlassungstatbestände wie z.B. Unterlassung der Vornahme einer Datenschutz-Folgenabschätzung (Art. 51 Abs. 1 lit. d. VE-DSG) oder Unterlassung betreffend Vorkehren „Privacy by Design" (Art. 51 Abs. 1 lit. e. VE-DSG). Äusserst fragwürdig ist – unter dem Blickwinkel von „nemo tenetur" – auch die Sanktionierung der Verletzung von Mitwirkungspflichten (Art. 50 Abs. 2 lit. c. VE DSG).
- Beachtung des Bestimmtheitsgebots: Nur Tatbestände, welche genügend klar umschrieben sind, können strafbewehrt werden.
- Die fahrlässige Tatbegehung darf nicht strafbar sein.
- Der heutige Art. 35 DSG (Verletzung der beruflichen Schweigepflicht) ist beizubehalten (anstelle Art. 52 VE-DSG): Es ist unverhältnismässig und nicht praktikabel, die Verletzung der beruflichen Schweigepflicht auf alle Personendaten auszudehnen (korrekterweise sind aktuell nur besonders schützenswerte Personendaten und Persönlichkeitsprofile erfasst) und mit einer Freiheitsstrafe von bis zu 3 Jahren zu bedrohen (aktuell Busse). Dies umso mehr, als – im Gegensatz zum Berufsgeheimnis im StGB – vorliegend nicht einmal eine Befreiung vom Berufsgeheimnis durch eine Aufsichtsbehörde vorgesehen ist und auch eine fahrlässige Tatbegehung strafbar wäre. Schliesslich müsste als Voraussetzung im Minimum eine berufliche Schweigepflicht unabhängig von Art. 52 VE-DSG bestehen (z.B. vertraglich), ansonsten so gut wie jeder Berufstätige eine strafrechtlich sanktionierte Schweigepflicht auferlegt bekäme.
- Keine Ausweitung von Art. 179novies StGB (bisher ist nur der Diebstahl von qualifizierten Daten sanktioniert), da die Abgrenzung von den sonstigen Datenschutzverletzungen unklar ist.

- Keine Verlängerung der Verfolgungsverjährung gegenüber der allgemeinen Regel im StGB: Art. 55 VE-DSG will die Verfolgungsverjährung für Übertretungen auf fünf Jahren ausdehnen, obschon Art. 109 StGB drei Jahre vorsieht.

Die KARTAC dankt Ihnen im Namen ihrer Mitglieder für die Entgegennahme und Prüfung unserer Ausführungen und Anliegen. Für Rückfragen und Erläuterungen stehen wir Ihnen gerne zur Verfügung

Freundliche Grüsse

KARTAC
Interessengemeinschaft der Zahlkartenindustrie

Uwe Behr
Präsident

Beat Steinmann
Sekretär

KONFERENZ DER KANTONALEN AUFSICHTSBEHÖRDEN IM ZIVILSTANDSDIENST
CONFÉRENCE DES AUTORITÉS CANTONALES DE SURVEILLANCE DE L'ÉTAT CIVIL
CONFERENZA DELLE AUTORITÀ CANTONALI DI VIGILANZA SULLO STATO CIVILE

Eidgenössisches Justiz- und
Polizeidepartement
Bundesamt für Justiz

Per Mail an:
jonas.amstutz@bj.admin.ch

Münsingen, 18. März 2017

Vernehmlassung des Bundes zur geplanten Totalrevision des Datenschutzgesetzes und die weiteren Erlasse zum Datenschutz (DSG)
Stellungnahme Konferenz der Kantonalen Aufsichtsbehörden im Zivilstandsdienst (KAZ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Brief vom 21. Dezember 2017 laden Sie in der eingangs erwähnten Angelegenheit zur Vernehmlassung ein. Wir wurden als betroffene Konferenz wiederholt nicht direkt bedient und figurierten nicht unter den Vernehmlassungsadressaten. Wir bitten Sie, uns künftig im Rahmen von Vernehmlassungen in Personenstandsangelegenheiten, Datenbekanntgabe und -bewirtschaftung, Registerfragen und dgl. wiederum direkt anzuschreiben, resp. uns in den entsprechenden Verzeichnissen aufzunehmen.

Gerne nehmen wir zur geplanten Totalrevision des DSG nachfolgend Stellung.

Zu Art. 2 Abs. 2 VE-DSG: Der Vorentwurf sieht eine Aufhebung der heute gültigen Ausnahme für öffentliche Register des Privatrechtsverkehrs vor (Art. 2 Abs. 2 Bst. d DSG). Wir halten diese Aufhebung für das eidgenössische Personenstandsregister (Infostar; Art. 39 und 45a ZGB) für nicht angebracht; die Konsequenzen sind aus unserer Sicht zu wenig durchdacht. Die Gleichsetzung von Infostar mit Zefix, dem Luftfahrzeugbuch und dem Markenregister auf Seite 41 des erläuternden Berichts zum Vorentwurf zur Totalrevision des DSG ist aus unserer Sicht nicht korrekt.

Es wird verkannt, dass die in Infostar geführten Daten höchst schützenswert sind, mehr noch als jene in Zefix und sicher weit mehr als jene in den anderen genannten Registern. Zudem können die Daten in Infostar, denen erhöhte Beweiskraft zukommt (Art. 9 ZGB), grundsätzlich nur in einem besonderen gerichtlichen Verfahren geändert werden (Art. 42 ZGB); bei den anderen genannten Registern können die Daten in einem einfachen Administrativverfahren geändert werden.

KAZ-GESCHÄFTSSTELLE
Sonnhaldeweg 3
3110 Münsingen
Tel. 079 785 88 45
E-Mail: info@kaz-zivilstandswesen.ch

Ferner wird verkannt, dass die heute geltenden Sonderbestimmungen und die damit verbundenen Abläufe beim Datenschutz von Zivilstandsdaten (Art. 43a ZGB in Verbindung mit Art. 44 ff. ZStV) über die heute geltenden Regelungen im DSG hinausgehen und seit Jahrzehnten bestens eingespielt sind; ein Reformbedarf ist nicht auszumachen. Es wäre fatal, für Zivilstandsdaten die gleichen Gesetzmässigkeiten vorzusehen, wie sie im VE zum DSG festgehalten sind. Eine Sonderregelung für Infostar wäre ohnehin unabdingbar, weshalb die Kann-Formulierung in Art. 45a Abs. 4 VE-ZGB (siehe dazu Seite 90 des erläuternden Berichts zum Vorentwurf zur Totalrevision des DSG) verfehlt ist.

Im Übrigen haftet der Unterscheidung zwischen öffentlichen Registern, für welche der Bund und für welche die Kantone zuständig sind, etwas Willkürliches an (die Daten des eidgenössischen Grundbuches zum Beispiel sollen weiterhin vom DSG ausgenommen werden, jene von Infostar aber nicht). Nicht einleuchtend ist in diesem Zusammenhang auch, dass Infostar zwar vom Bund (künftig) geführt wird, die Kantone aber weiterhin für Schaden aufkommen sollen, welcher aus der Führung des Personenstandsregisters entsteht (Art. 46 Abs. 2 ZGB); auch die Haftung müsste unserer Meinung nach auf den Bund übergehen (mit entsprechender Anpassung von Art. 46 Abs. 2 ZGB).

Zu Art. 45a Abs. 3 und 4 VE-ZGB: Der erläuternde Bericht zum Vorentwurf zur Totalrevision des DSG und zur Teilrevision des ZGB äussert sich nicht dazu, ob und welche Aufgaben den kantonalen Datenschutzbehörden im Zusammenhang mit der Beurkundung des Personenstandes neu zukommen sollen. Auf Seite 90 des erläuternden Berichts wird nur gerade ausgeführt, dass «… die kantonalen Datenschutzbehörden und der Beauftragte im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammenarbeiten und für eine koordinierte Aufsicht über die Bearbeitung von Personendaten sorgen.». Warum den kantonalen Datenschutzbehörden bei den Daten in Infostar eine Aufsichtsfunktion zukommen soll, nachdem die Ausnahme in Art. 2 Abs. 2 Bst. d DSG für Infostart neu nicht mehr gelten soll (Art. 2 Abs. 2 VE-DSG), ist nicht nachvollziehbar. Konsequenterweise dürfte bei den Daten in Infostar neu nur dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten eine Aufsichtsfunktion zukommen.

Zu wenig durchdacht scheint uns auch die Abgrenzung zwischen den Aufgaben der kantonalen Aufsichtsbehörden im Zivilstandswesen (Art. 45 ZGB) und den kantonalen Datenschutzbehörden bzw. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. Bezogen auf den Datenschutz bzw. die Bekanntgabe von Zivilstandsdaten kommen den kantonalen Aufsichtsbehörden im Zivilstandswesen heute zahlreiche Aufgaben zu (Art. 45 Abs. 2, Art. 46, Art. 46a, Art. 50 Abs. 3, Art. 60 Abs. 1 ZStV). Aus unserer Sicht sind mit der vorgeschlagenen Neuregelung Kompetenzkonflikte zwischen den kantonalen Aufsichtsbehörden im Zivilstandswesen, welche heute für den Schutz der beurkundeten Daten besorgt sind, und den kantonalen Datenschutzbehörden bzw. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten bereits vorprogrammiert.

Die Unzweckmässigkeit der Kann-Vorschrift in Art. 45a Abs. 4 VE-ZGB haben wir bereits erörtert. Wenn es bei der Aufhebung der heute gültigen Ausnahme für Infostar (Art. 2 Abs. 2 Bst. d DSG) bleiben sollte, schlagen wir mindestens eine bindende Verpflichtung des Bundesrates zur abweichenden Reglung der Ansprüche der betroffenen Personen vor.

KAZ-GESCHÄFTSSTELLE
Sonnhaldeweg 3
3110 Münsingen
Tel. 079 785 88 45
E-Mail: info@kaz-zivilstandswesen.ch

Wir danken Ihnen bestens für die Berücksichtigung unserer Eingabe.

Freundliche Grüsse

KONFERENZ DER KANTONALEN AUFSICHTSBEHÖRDEN IM ZIVILSTANDSDIENST

Namens des Vorstandes

Die Präsidentin:

Esther Gassler, Regierungsrätin

Der Geschäftsführer:

Walter Grossenbacher

Kopie an

- alle Kantone, z.H. der für den Zivilstandsdienst zuständigen Regierungsmitglieder und die kantonalen Aufsichtsbehörden

KAZ-GESCHÄFTSSTELLE
Sonnhaldeweg 3
3110 Münsingen
Tel. 079 785 88 45
E-Mail: info@kaz-zivilstandswesen.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : KünzlerBachmann Directmarketing AG

Abkürzung der Firma / Organisation : kbdirect

Adresse : Zürcherstrasse 601, 9015 St. Gallen

Kontaktperson : Roger Muffler

Telefon : 071 314 04 21

E-Mail : r.muffler@kbdirect.ch

Datum : 31.03.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
kbdirect	Kbdirect begrüsst die Revision des Datenschutzgesetzes und die damit verbundenen Zielsetzungen. Datenschutzrechtliche Fragestellungen werden bei der fortschreitenden Digitalisierung nicht nur beim Geschäftsmodell von kbdirect zunehmend an Bedeutung gewinnen. Wichtig ist hierbei für alle Anspruchsgruppen eine grosse Rechtssicherheit betreffend den Umgang mit Personendaten. In diesem Punkt sehen wir einige der vorgeschlagenen Regelungen kritisch. Dies insbesondere auch mit Blick auf die zu erwartenden Sanktionen. Wenn die Nicht-Einhaltung einer Pflicht mit einer Sanktion bedroht werden soll, muss für die Datenbearbeiter genügend bestimmbar sein, in welchen Konstellationen die betreffende Pflicht ausgelöst wird und was zur Umsetzung der Pflicht getan werden muss. Die Regelungen im Datenschutz sollen die Interessen der betroffenen Personen schützen, gleichzeitig aber sinnvolle, digitale und andere Geschäftsmodelle nicht unnötig beeinträchtigen. Hierbei ist zu berücksichtigen, dass in der digitalen Wirtschaft grenzüberschreitende Datenbearbeitungen alltäglich sind. Die schweizerische Datenschutzgesetzgebung darf damit auch nicht zu Wettbewerbsnachteilen für schweizerische Unternehmen, insbesondere KMU führen. Das Geschäftsmodell von Kbdirect ist besonders data-driven. Es umfasst die zielgerichtete und fokussierte Werbung mittels Datenselektion und analytischen Verfahren. Die Dienstleistungen von Kbdirect helfen Unternehmen und Organisationen - darunter zahlreiche Schweizer KMU und Spendenorganisationen - dabei, ihre bestehenden Kunden effizienter und zielgerichteter anzusprechen und neue Kunden zu gewinnen. Die Kommunikation zwischen Unternehmen und deren aktuellen und potenziellen Kunden ist für jedes Unternehmen der Sauerstoff für den wirtschaftlichen Erfolg. Die zielgerichtete Werbung bringt jedoch auch den betroffenen Personen einen Mehrwert. Durch die Personalisierung erhalten die betroffenen Personen Informationen zu Produkten oder Dienstleistungen, welche sie interessieren, d.h. welche relevant sind. Im Zusammenhang mit der Adressselektion für Spendenorganisation wird zudem sichergestellt, dass potenzielle Spender effizient mit passenden Spendenorganisationen zusammengebracht werden. Es ist unbestritten, dass personalisierte Marketingkommunikation für die Wirtschaft, insbesondere auch für kleinere KMU, wichtig ist. Es besteht damit ein berechtigtes und substantielles Interesse an den Dienstleistungen von Kbdirect und anderen Unternehmen mit vergleichbarem Geschäftsmodell. Die EU-DSGVO anerkennt dieses Interesse (vgl. z.B. RZ 47, S. 9 DSGVO, letzter Satz). Informationspflichten, Regelungen zum Profiling sowie Sorgfaltspflichten können, je nach Ausgestaltung, die effiziente Form von Werbung erschweren oder teilweise gar verunmöglichen. Sehen andere Länder weniger einschränkende Regelungen für den Datenschutz im Bereich der personalisierten Werbung vor, entsteht für schweizerische Unternehmen wie kbdirect ein Wettbewerbsnachteil. Ein Wettbewerbsnachteil ergibt sich jedoch nicht nur für kbdirect, sondern auch für deren Kunden, d.h. die Unternehmen und Organisation, deren Kommunikation mit bestehenden und vor allem potenziellen Kunden

	erschwert wird. Vor diesem Hintergrund lehnen wir im Grundsatz jeden Swiss Finish ab. Die Revision des Datenschutzgesetzes soll sich auf die Einhaltung der Vorgaben der Europarats-Konvention (E-SEV 108) und die Angemessenheit im Hinblick auf die EU beschränken. Den „Swiss Finish“ bei einzelnen Regelungen (z.B. beim Profiling und bei der Sanktionierung von Verstössen) lehnen wir strikte ab. In der aktuellen Fassung müssen wir den vorgelegten Vorentwurf des neuen DSG ablehnen. Insbesondere das vorgesehene Sanktionssystem, mit dem eine weitgehende Kriminalisierung von natürlichen Personen in den datenbearbeitenden Unternehmen erfolgt, ist inakzeptabel.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
kbdirect	DSG	3		a	Wir begrüssen, dass keine Änderung am Begriff der „Personendaten“ vorgenommen wird. Die Ausführungen zu Art. 3 lit. a VE-DSG im erläuternden Bericht könnten allerdings zu Diskussionen führen. Es wurden dort, praktisch eins zu eins, die Erwägungsgründe aus der EU-DSGVO übernommen, welche in der EU zu Unklarheiten geführt haben. Wir sind der Meinung, dass dann, wenn keine inhaltliche Änderung vorgesehen ist, in den Materialien nicht aus der EU-DSGVO zu zitieren ist. Vielmehr ist auf die bisherige Praxis und Rechtsprechung in der Schweiz zu verweisen, z.B. auf den Logitech-Entscheid des Bundesgerichtes. Entscheidend ist aus unserer Sicht vor allem, dass die sog. relative Methode betreffend die Bestimmbarkeit einer natürlichen Person explizit anerkannt wird.
kbdirect	DSG	3		f	**Wir lehnen die vorgeschlagene Definition und die damit einhergehende Regelung (siehe dazu Anmerkungen zu Art. 23 unten) des „Profiling“ ausdrücklich ab. Die Regelung geht ohne Not über diejenige der EU-DSGVO (Art. 4 Ziff. 4) hinaus (Swiss Finish).** Die E-SEV 108 verlangt die vorgeschlagene Regelung ebenfalls nicht. Bei der Definition im Gesetz bzw. in den Materialien ist konkreter zu bestimmen, wann ein Profiling vorliegt. Für die Rechtsanwender ist aktuell vollkommen unklar, wann ein Profiling im Sinne des Vorschlags vorliegt. Dies ist gerade für Unternehmen wie kbdirect problematisch. Bei der aktuellen Definition und den Ausführungen im erläuternden Bericht könnte jede irgendwie geartete Analyse oder Auswertung betreffend die wirtschaftliche Leistung, etc. als Profiling gelten. In der Praxis gibt es jedoch z.B. grosse Unterschiede bei der Bewertung der Kaufkraft einer Person. Für die

					Persönlichkeit einer betroffenen Person macht es einen Unterschied, ob die Kaufkraft z.B. annäherungsweise aus dem Wohnort, Beruf und der Wohnsituation berechnet wird oder z.B. anhand von Wirtschaftsdaten, die über eine längere Zeit erhoben werden. Der Begriff des Profiling ist sodann auf automatisierte Bearbeitungen zu beschränken. Bei manuellen Bearbeitungen könnte es zwar theoretisch auch zu grösseren Auswertungen kommen, doch sind die Risiken für die Persönlichkeit als gering einzuschätzen. Die Datenbearbeitungsgrundsätze reichen hierbei ohne Weiteres aus. Zu streichen ist auch die Unterscheidung zwischen Personendaten und Daten, d.h. nicht personenbezogenen Daten. Diese Unterscheidung führt lediglich zu Unklarheiten und Missverständnissen.
kbdirect	DSG	4	3		Die „klare“ Erkennbarkeit ist zu streichen. Wie der erläuternde Bericht zu Recht festhält, ist eine inhaltliche Änderung des Zweckbindungsgebotes nicht beabsichtigt und auch nicht notwendig. Der Verweis auf die „klare“ Erkennbarkeit führt lediglich zu Missverständnissen. Zu Missverständnissen hat im deutschen Wortlaut auch geführt, dass nur von einem Zweck die Rede ist. Da gegenüber dem geltenden Recht keine inhaltliche Änderung geplant ist, müssen Daten auch für mehr als einen Zweck bearbeitet werden können, sofern alle diese Zwecke transparent gemacht werden. Dies ist entweder im Wortlaut der Bestimmung oder in den Materialien explizit festzuhalten.
kbdirect	DSG	4	5		Gemäss Seite 47 des erläuternden Berichts sind keine materiellen Änderungen beabsichtigt. Es gibt keinen Grund dafür, den Wortlaut zu ändern. Dies führt lediglich zu Missverständnissen und Unklarheiten. Für die Einhaltung der E-SEV 108 sowie für die Angemessenheit im Vergleich mit der EU-DSGVO sind terminologische Annäherungen nicht massgeblich. Entscheidend ist der Inhalt

					und die Handhabung in der Praxis.
kbdirect	DSG	4	6		**Auch betreffend die Begriffsbestimmung der „Einwilligung" ist nicht ersichtlich, weshalb eine terminologische Annäherung notwendig sein soll, wenn sich inhaltlich an der Einwilligung nichts ändert**. Sofern sich an einer Bestimmung inhaltlich nichts ändern soll, ist der Wortlaut im Vergleich zum geltenden DSG nur ausnahmsweise anzupassen. Vorliegend ist damit auf eine Änderung zu verzichten. Die terminologische Änderung könnte gerade bei der Einwilligung zu Unklarheiten führen. Die strengen Voraussetzungen an die Einwilligung in der EU-DSGVO werden primär aus dem Gesetzeswortlaut abgeleitet. Mit der Übernahme eines vergleichbaren Wortlautes wie in der EU-DSGVO könnten sich damit auch inhaltliche Auslegungsfragen ergeben. Dies ist jedoch explizit nicht geplant. Wird die vorgeschlagene Terminologie beibehalten, ist in den Materialien explizit klarzustellen, dass sich inhaltlich an der Interpretation des Begriffes „Einwilligung" und an den Anforderungen an diese gegenüber dem geltenden DSG nichts ändert. Unklar bzw. unbestimmt und widersprüchlich sind sodann die Ausführungen im erläuternden Bericht zur ausdrücklichen Einwilligung. Dies wiegt vorliegend beim Geschäftsmodell von kbdirect insofern schwer, als z.B. das Profiling ohne ausdrückliche Einwilligung grundsätzlich eine Persönlichkeitsrechtsverletzung darstellt. Der Umstand, dass sowohl „Profiling" als auch „ausdrückliche Einwilligung" nicht zweifelsfrei bestimmt sind, führt beim Rechtsanwender zu einer inakzeptablen Rechtsunsicherheit. Diese Rechtsunsicherheit schadet auch der betroffenen Person, da wegen dieser Rechtsunsicherheit allenfalls auf Datenbearbeitungen verzichtet wird, welche im Interesse der betroffenen Personen wären. In den Materialien ist zuletzt auch klarzustellen, dass die Einwilligung – auch die ausdrückliche – wie bisher auch durch Zustimmung zu einem Dokument erteilt werden kann, in welchem auch weitere Informationen enthalten sind (z.B. AGB

					oder Datenschutzerklärungen). Es gibt keinen Grund, von der entsprechenden Praxis unter dem geltenden Datenschutzgesetz bzw. der geltenden Regelung und Praxis im schweizerischen Obligationenrecht abzuweichen.
kbdirect	DSG	5 + 6			**Bei den Regelungen zur Bekanntgabe von Daten ins Ausland handelt es sich um einen Swiss Finish.** Auf diesen ist zu verzichten. Zur Einhaltung der E-SEV 108 ist unseres Erachtens keine inhaltliche Änderung der Datentransfer-Regelung im bestehenden DSG notwendig. Auch die EU-DSGVO bzw. die Sicherstellung der Angemessenheit zum betreffenden Datenschutzstandard verlangt keine solch komplizierte Umsetzung. Die vorgeschlagene Regelung ist für den Schutz der betroffenen Personen unnötig und führt vielmehr im Geschäftsalltag zu erheblichen Beeinträchtigungen. In den Konstellationen, in denen die vorgeschlagene Regelung eine Genehmigung des EDÖB vorsieht, würde der – regelmässig sinnvolle – Datentransfer ins Ausland zeitlich unnötig aufgehalten, ohne dass für die betroffenen Personen ein besserer Schutz erzielt wird. Unnötig – und auch durch die EU-DSGVO nicht gefordert – ist die generelle Informationspflicht bei der Nutzung von standardisierten Garantien (Art. 5 Abs. 6 VE-DSG). Es geht hierbei um die Nutzung von Garantien, welche durch den EDÖB anerkannt bzw. genehmigt wurden. Zuletzt ist in Art. 6 Abs. 1 lit. a VE-DSG der Zusatz „im Einzelfall“ zu streichen. Bei wiederkehrenden Sachverhalten und unveränderter Erkennbarkeit und Erwartung muss eine einmalige Zustimmung ausreichen.
kbdirect	DSG	7			**Auch bei der vorgeschlagenen Regelung zur Auftragsbearbeitung handelt es sich um einen Swiss Finish**. Die bestehende Regelung würde für die Einhaltung der E-SEV 108 ausreichen. Für die Angemessenheit würde die bestehende Regelung ebenfalls ausreichen. Die vorgeschlagenen Anforderungen – insbesondere betreffend den Beizug von

					Subunternehmern – führen im wirtschaftlichen Alltag zu unnötigen Beeinträchtigungen. Die Auftragsbearbeitung ist in einer arbeitsteiligen, globalen Wirtschaft wie der schweizerischen absolut bedeutsam und für alle Wirtschaftsakteure wichtig. Es ist nicht ersichtlich, weshalb daher die Auftragsbearbeitung unnötig belastet werden soll. Die betroffenen Personen gewinnen durch die vorgeschlagenen Regelungen im Vergleich zum bestehenden DSG nichts. Für die betroffenen Personen ist entscheidend, dass der Verantwortliche für alle Auftragsdatenbearbeitungen letztverantwortlich bleibt. Sie können sich in jedem Fall an den Verantwortlichen wenden. Es liegt in der Eigenverantwortung des Verantwortlichen, wie er diese Verantwortung wahrnimmt und die Kontrolle über die Auftragsbearbeitungen sicherstellt. Zuletzt ist die unbeschränkte Delegation zur Festlegung weiterer Pflichten an den Bundesrat zu streichen. Diese Kompetenzdelegation führt zu Rechtsunsicherheit. Es bestünde die Gefahr, dass der Bundesrat in einem Bereich reguliert, der bis anhin unter dem geltenden Datenschutzrecht nicht zu Problemen geführt hat.
kbdirect	DSG	8			Kbdirect begrüsst die Einführung von Empfehlungen der guten Praxis. Dies bringt zusätzliche Rechtssicherheit, was bei der zunehmenden Komplexität der Datenbearbeitungen wichtig ist. Kbdirect wehrt sich jedoch dagegen, dass der EDÖB quasi ein Letztgenehmigungsrecht erhält. Das Genehmigungsrecht ist einer neutralen Instanz zuzuweisen. Dies auch aus rechtsstaatlichen Gesichtspunkten – Stichwort Gewaltenteilung. Die Empfehlungen dürften aufgrund der vorgeschlagenen Regelung bis zu einem gewissen Grad gesetzesergänzende Wirkung erhalten. Beim EDÖB handelt es sich dagegen primär um eine gesetzesvollziehende Behörde. Der Anstoss für solche Empfehlungen muss zwingend aus der Praxis und den Verbänden kommen. Sollte das Letztgenehmigungsrecht des EDÖB beibehalten bleiben, muss zumindest klargestellt werden, dass der EDÖB selber keine

					Empfehlungen vorschlagen, sondern diese nur genehmigen kann.
kbdirect	DSG	8	1		Kbdirect ist der Auffassung, dass gegen Empfehlungen der guten Praxis, d.h. den Erlass oder die Nicht-Genehmigung solcher Empfehlungen, ein Rechtsmittelweg offenstehen muss. Dieser Rechtsmittelweg ist im Gesetz zu regeln. Ein Rechtsmittel ist insbesondere dann von grosser Bedeutung, wenn die Empfehlungen durch den EDÖB genehmigt werden oder wenn, was zu vermeiden ist, der EDÖB auch selber solche Empfehlungen entwerfen und lancieren darf.
kbdirect	DSG	8	2		Es kann auf die vorangehende Bemerkung verwiesen werden. Wichtig sind Rechtsmittel gegen Genehmigungen bzw. Nicht-Genehmigungen von Empfehlungen.
kbdirect	DSG	12			**Bei dieser Regelung handelt es sich um einen Swiss Finish**. Eine entsprechende Regelung ist weder durch die E-SEV 108 noch die EU-DSGVO vorgesehen. Das Datenschutzgesetz ist der falsche Ort für eine solche Regelung. Die vorgeschlagene Bestimmung ist ersatzlos zu streichen.
kbdirect	DSG	13			Es ist fraglich, ob die vorgeschlagene aktive Informationspflicht gegenüber der Transparenzpflicht im geltenden DSG für die betroffenen Personen überhaupt zu einem Mehrwert führt. Da die E-SEV 108 und auch die EU-DSGVO eine solche Informationspflicht im Grundsatz vorsehen, ist die Diskussion darüber müssig. **Bei der Ausgestaltung der Informationspflicht und vor allem bei den Anforderungen an deren Umsetzung ist allerdings im Auge zu behalten, dass diese Pflicht die Transparenz der Datenbearbeitungen fördern soll, was bereits nach geltendem Recht sicherzustellen ist.** Die Informationspflicht ist auf diejenigen Angaben zu beschränken, welche für die Transparenz notwendig sind. Die zu liefernden Informationen sind abschliessend zu bestimmen. Offene Rechtsbegriffe oder Umschreibungen der Pflicht sind zu vermeiden. Dies auch deshalb, weil die Verletzung der Informationspflicht mit

					Sanktionen bedroht ist. Klarzustellen ist in den Materialien, wie die Informationspflicht umzusetzen ist. In den Materialien ist diesbezüglich explizit darauf hinzuweisen, dass die Information auch in Form von standardisierten Datenschutzerklärungen auf der Webseite erfüllt werden kann. Es muss hierbei, wie nach geltendem Recht, genügen – und dies ist in den Materialien ebenfalls klarzustellen –, dass z.B. bei einem Bestellformular oder einer Bestellkarte auf diese Datenschutzerklärungen auf der Webseite verwiesen werden kann und die Datenschutzerklärung nicht vollständig auf die Bestellkarte abgedruckt werden muss. Der Explanatory Report zur betreffenden Pflicht in der E-SEV 108 verweist ebenfalls darauf, dass die Information in einer Datenschutzerklärung auf der Webseite enthalten sein kann. Des Weiteren ist klarzustellen, dass die Informationspflicht sich auf Angaben bezieht, die im Zeitpunkt der Datenbeschaffung bestehen bzw. bekannt sind. Der vorgeschlagene Wortlaut sagt klar, dass die Information spätestens im Zeitpunkt der Datenbeschaffung erfolgen muss. Eine spätere Neuinformation ist, wie unter geltendem Recht, nicht notwendig bzw. müsste sich aus einer anderen Bestimmung des DSG (z.B. dem Transparenzgebot) ergeben.
kbdirect	DSG	13	3		Wegen der Sanktionsdrohung muss die Auflistung der Informationen abschliessend sein. Eine andere Regelung würde dazu führen, dass die Unternehmen zur Sicherheit über alles Mögliche informieren, was die Transparenz für die betroffene Person vermindern würde. Die betroffene Person muss primär wissen, von wem, welche Daten für welche Zwecke bearbeitet werden. Dadurch kann sich die betroffene Person einen ersten Überblick schaffen und, falls notwendig, über das Auskunftsrecht zusätzliche Informationen beschaffen.
kbdirect	DSG	13	4		**Es handelt sich hierbei um einen unnötigen Swiss Finish, der zu streichen ist**. Es ist insbesondere nicht ersichtlich, weshalb die Angabe der Kategorien von Auftragsbearbeitern nicht genügen sollte. Für die betroffene Person ist es einzig

					wichtig, dass der Verantwortliche eine korrekte Datenbearbeitung durch die Auftragsbearbeiter sicherstellt.
kbdirect	DSG	13	5		Die Ausdehnung der Pflicht auf die indirekte Datenbeschaffung wird in der Praxis jegliche Beschaffung von Daten bei Dritten verunmöglichen. Die Bestimmung ist zu streichen. Wie bereits erwähnt, sind kbdirect und vor allem auch deren Kunden auf die Beschaffung von Daten aus Drittquellen angewiesen. Nur so entsteht Potenzial für die Kommunikation mit möglichen neuen Kunden. Die zielgerichtete Ansprache von neuen Kunden ist im verschärften Wettbewerb, in dem sich schweizerische Unternehmen, KMUs wie auch Grosskonzerne, befinden, von elementarer Bedeutung. **Sollte an der Informationspflicht bei der indirekten Datenbeschaffung festgehalten werden, ist die Regelung anzupassen. Beim Vorschlag handelt es sich um einen Swiss Finish.** Bei der E-SEV 108 ist im Explanatory Report zur betreffenden Regelung vorgesehen, dass die Information zeitlich verzögert werden kann und z.B. erst erfolgen muss, wenn das Unternehmen mit der betroffenen Person kommuniziert. Auch die EU-DSGVO lässt eine zeitliche Verzögerung zu. Im Gegensatz dazu sieht der VE-DSG die Information bereits im Zeitpunkt der Speicherung der Personendaten vor. Aus dem Vorentwurf und dem erläuternden Bericht geht zudem nicht hervor, wie die Informationspflicht bei der indirekten Beschaffung umzusetzen ist. Wie bei der Informationspflicht bei der direkten Beschaffung muss es möglich sein, die Detailinformationen in einer standardisierten Datenschutzerklärung auf der Webseite aufzuführen.
kbdirect	DSG	14	4	a	**Der Katalog der Ausnahmen ist enger gefasst, als es nach dem E-SEV 108 erforderlich wäre (Swiss Finish)**. Der Ausnahmekatalog soll daher mindestens die Ausnahmen gemäss E-SEV 108 enthalten.
kbdirect	DSG	15			Der Anwendungsbereich der vorgeschlagenen Regelung geht zu weit. Es ist

					klarzustellen, **dass auch rechtliche Auswirkungen eine gewisse Schwere erreichen müssen.** Praktisch jeder Entscheid kann rechtliche Wirkungen haben. Art. 22 EU-DSGVO sieht zudem betreffend automatisierte Einzelfallentscheidungen Ausnahmen vor (z.B. wenn die automatisierte Einzelfallentscheidung für die Abwicklung eines von der betroffenen Person gewünschten Vertrages notwendig ist). Die E-SEV 108 würde solche Ausnahmen zulassen. Diese sind damit auch in Art. 15 DSG aufzunehmen.
kbdirect	DSG	16			**Die vorgeschlagene Regelung zur Datenschutz-Folgenabschätzung stellt ebenfalls einen Swiss Finish dar, auf den zu verzichten ist.** Die vorgeschlagene Regelung könnte theoretisch dazu führen, dass selbst eine einzelne Datenbekanntgabe ins Ausland zu einer Folgenabschätzung und Notifikation an den EDÖB führt. Dies führt zu einer unnötigen Belastung der Unternehmen und auch des EDÖB. Die Regelung muss so ausgestaltet werden, dass nur Datenbearbeitungsprozesse, welche regelmässig durchgeführt werden, eine Datenschutz-Folgenabschätzung auslösen können. Art. 35 EU-DSGVO erwähnt z.B. die systematische Bearbeitung besonders schützenswerter Daten oder das umfangreiche Profiling. Entsprechend der EU-Regelung **sollten damit nur regelmässige Datenbearbeitungen mit „hohem Risiko" (oder besser „besonders hohem Risiko") Prüfungsgegenstand sein**. Wie in der EU-DSGVO sollte der EDÖB zudem dazu verpflichtet werden, eine Positiv- oder Negativliste mit den Datenbearbeitungen zu erstellen, bei denen eine Datenschutz-Folgenabschätzung notwendig ist. Dies ist auch deshalb wichtig, weil die Verletzung der Pflicht zur Datenschutz-Folgenabschätzung sanktioniert werden soll. Der EDÖB kann sich an den Listen orientieren, welche durch die EU-Datenschutzbehörden erstellt werden müssen. **Die vorgeschlagene Regelung geht in weiteren Punkten über die EU-DSGVO hinaus (Swiss Finish)**: Art. 35 DSGVO beschränkt die Pflicht auf den

					Verantwortlichen, während Art. 16 VE-DSG vom Verantwortlichen und vom Auftragsbearbeiter spricht. Die E-SEV 108 sieht ebenfalls nicht vor, dass der Auftragsbearbeiter eine Datenschutz-Folgenabschätzung durchführen muss. Die vorgeschlagene Ausdehnung der Pflicht auf den Auftragsbearbeiter ist damit zu streichen. **Bei der Notifikationspflicht an den EDÖB handelt es sich ebenfalls um einen unnötigen Swiss Finish**. Art. 36 EU-DSGVO verlangt eine Notifikation nicht bei jeder Datenschutz-Folgenabschätzung, sondern nur dann, wenn die Prüfung effektiv ein hohes Risiko ergab **und** wenn der Verantwortliche keine Massnahmen zur Risikoreduktion treffen will oder kann. Die Ausgestaltung der Notifikationspflicht in Art. 36 EU-DSGVO ist für die Schweiz zu übernehmen. Zudem ist die Reaktionsfrist des EDÖB zu verkürzen.
kbdirect	DSG	17			**Bei diesem Vorschlag handelt es sich um ein schweizerisches Überschiessen (Swiss Finish).** Wie im E-SEV 108 (Art. 7 Abs. 2) vorgesehen**,** ist die Meldepflicht auf Verletzungen zu beschränken, welche die Rechte der Betroffenen „schwerwiegend" („seriously") gefährden könnten. **Die Meldepflicht an die betroffene Person ist gänzlich zu streichen**. Eine solche Pflicht ist im E-SEV 108 nicht zwingend vorgesehen.
kbdirect	DSG	18			Die Anforderungen an die Datenbearbeiter durch diese beiden Pflichten sind unklar. Weder aus dem Wortlaut noch aus dem erläuternden Bericht geht hervor, was für Vorkehrungen zu treffen sind. Dies ist umso schwerwiegender als die Verletzung dieser Bestimmung mit Strafe bedroht ist. Auch wenn gewisse Details in Empfehlungen der guten Praxis geregelt werden können, müssen die Grundsatzfragen, insbesondere die grundsätzlichen Anforderungen im Gesetz geregelt werden. Im Zweifelsfalle, d.h. ist es nicht möglich, die Pflichten klarer zu umschreiben, ist auf eine Sanktionierung zu verzichten. Eine indirekte Sanktionierung kann immer noch dadurch erfolgen, dass der EDÖB nach erfolgter Untersuchung Empfehlungen abgibt oder die

					Implementierung gewisser Massnahmen verfügt. Hält sich der Datenbearbeiter nicht an diese Empfehlung oder Verfügung, kann diese Widerhandlung sanktioniert werden.
kbdirect	DSG	19		a	Aufgrund des vorgeschlagenen Gesetzeswortlautes und des erläuternden Berichts ist der Umfang der Dokumentationspflicht unklar. Im Gesetz ist konkreter festzulegen, welche Angaben über eine Datenbearbeitung dokumentiert werden müssen. Zudem ist klarzustellen, dass es sich dabei nicht um die Dokumentation einer einzelnen Datenbearbeitung handeln kann. Ansonsten würde die Dokumentationspflicht, insbesondere für kleinere Unternehmen zu einem unnötigen Aufwand führen. Wie in der EU-DSGVO vorgesehen, sollte sich die Dokumentationspflicht auf strukturierte Datensätze beschränken. Zudem sind, wie in der EU-DSGVO Ausnahmen von der Dokumentationspflicht vorzusehen. Nachdem die Dokumentationspflicht die Pflicht zur Anmeldung einer Datensammlung ersetzen und gemäss Regulierungsfolgeabschätzung durch diese Neuregelung kein zusätzlicher administrativer Aufwand entstehen soll, sollten die Angaben, welche damals bei der Anmeldung der Datensammlung bekannt gegeben werden mussten, auch für die Dokumentationspflicht genügen.
kbdirect	DSG	19		b	**Eine solche Mitteilungspflicht ist im E-SEV 108 nicht zwingend vorgesehen (Swiss Finish). Sie ist deshalb ersatzlos zu streichen.** Sofern an der Pflicht festgehalten wird, soll sie nur dann ausgelöst werden, wenn die betroffene Person dies verlangt und ein berechtigtes Interesse geltend machen kann. Es kann z.B. Konstellationen geben, in denen es gar nicht im Interesse der betroffenen Person ist, wenn gemäss Vorschlag Dritte informiert werden.
kbdirect	DSG	20	1		**E-SEV 108 verlangt nicht, dass die Ausübung des Auskunftsrechts kostenlos sein muss.** Es wird nur verlangt, dass die Auskunftserteilung ohne übermässige Kosten erfolgen muss („without excesive expense“; Art. 8 Abs. 1 lit.

					b). Eine angemessene Aufwandsentschädigung ist damit weiterhin zulässig.
kbdirect	DSG	20	3		**Es handelt sich wiederum um einen unnötigen Swiss Finish, der mit viel administrativem Aufwand für die Unternehmen verbunden ist.** Entsprechend der Regelung in der EU-DSGVO (Art. 15 Abs. 1 lit. h) ist das Auskunftsrecht auf diejenigen Fälle zu beschränken, in welchen auch eine Informations- und Anhörungspflicht nach Art. 15 VE-DSG besteht, also auf Entscheidungen, die automatisiert erfolgen und entsprechende Auswirkungen haben.
kbdirect	DSG	23	2	d	Wie bereits erwähnt, ist aufgrund der vorgeschlagenen Begriffsbestimmung des Profiling unklar, wann eine solche Tätigkeit vorliegt. Kbdirect bildet z.B. mithilfe von verschiedenen „normalen“ Daten sog. Selektionsvariabeln. Diese Variabeln entstehen nicht zwingend durch statistisch-mathematische Verfahren oder durch Big-Data-Analysen. Gleichwohl kann z.B. eine dieser Variabeln die Kaufkraft sein, welche jedoch nicht statistisch-mathematisch aufgrund der Auswertung von grösseren Datenmengen ermittelt wird, sondern vielmehr durch eher statische allgemeine Informationen. Es ist aufgrund der vorgeschlagenen Begriffsbestimmung unklar, ob hier bereits ein Profiling vorliegt. Wenn zudem für dieses Profiling eine ausdrückliche Einwilligung notwendig ist, wirkt sich diese begriffliche Unklarheit auf kbdirect, aber auch viele andere Unternehmen, erschwerend aus. Es ist hierbei zu beachten, dass personalisiertes Marketing auch im Interesse der betroffenen Personen ist. Zudem schadet eine unnötige Erschwerung auch der Wirtschaft. Insbesondere KMUs sind auf gute und effiziente Marketingmöglichkeiten angewiesen, um sich auf dem Markt sichtbar zu machen. **Das Erfordernis der ausdrücklichen Einwilligung für das Profiling ist daher zu streichen. Es handelt sich hierbei um einen Swiss Finish**. Weder E-SEV 108 noch die EU-DSGVO sehen eine solche Regelung vor. Für den Schutz der

					betroffenen Person genügt es, wenn die Datenbearbeitungsgrundsätze eingehalten werden. **Wird diese Vorschrift Gesetz, verunmöglicht sie einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar**. Profitieren würden die (häufig) ausländischen Unternehmen, bei denen die Nutzer jeweils einen Account eröffnen müssen. Im Rahmen der Account-Eröffnung können diese Unternehmen die ausdrückliche Einwilligung problemlos einholen. Die vielleicht gutgemeinte Regelung würde dadurch den Schutz der betroffenen Personen nicht wesentlich erhöhen, dafür aber schweizerische KMUs gegenüber ausländischen Giganten benachteiligen.
kbdirect	DSG	23	3		Die Beibehaltung dieser Regelung ist für kbdirect und andere Unternehmen, welche veröffentlichte Daten beschaffen, wichtig. Im erläuternden Bericht wurde jedoch unnötig für Unklarheit gesorgt. Statt einem blossen Verweis auf die bisherige Praxis wurde angefügt, dass die Datenbearbeitung rechtmässig sein muss. Dies ist nach geltendem Recht nicht zwingend der Fall.
kbdirect	DSG	25			**Der letzte Satz in Absatz 2 ist ersatzlos zu streichen**. Es handelt sich um einen Swiss Finish. Weder die E-SEV 108 noch die DSGVO sehen vor, dass neben dem Bestreitungsvermerk auch eine Beschränkung der Datenbearbeitung verlangt werden kann.
kbdirect	DSG	44	3		**Gegen vorsorgliche Massnahmeverfügungen des EDÖB sind Rechtsmittel mit aufschiebender Wirkung zur Verfügung zu stellen.** Die Massnahmen können bei den Unternehmen zu erheblichen Schäden führen. Die bisherige Praxis zeigt, dass vorsorgliche Massnahmen des EDÖB immer wieder mal vom Bundesverwaltungsgericht aufgehoben wurden.
kbdirect	DSG	50 ff.			**Kbdirect lehnt die vorgeschlagene Sanktionsregelung strikte ab. Diese**

					Regelung ist so weder in der E-SEV 108, noch in der EU-DSGVO vorgesehen. Die vorgeschlagene Sanktionsregelung führt dazu, dass die für Datenbearbeitungen verantwortlichen Personen in den Unternehmen direkt mit Strafrisiken bedroht sind. Die subsidiäre Haftung des Unternehmens dürfte gerade bei kleineren Unternehmen, bei denen die verantwortliche Person relativ leicht eruiert werden kann, kaum zur Anwendung gelangen. Die Strafrisiken für die verantwortlichen Personen würden dazu führen, dass kein Mitarbeiter mehr bereit wäre, die Funktion eines internen Datenschutzbeauftragten zu übernehmen. Der interne Datenschutzbeauftragte wird für die Datenschutz-Compliance in Zukunft jedoch besonders wichtig werden. Dies auch wenn der Vorentwurf – zu Recht – keine zwingende Pflicht zur Ernennung eines solchen Beauftragten vorsieht. Zudem würde die Strafbarkeit der Mitarbeiter dazu führen, dass diese – allenfalls vorschnell – Verstösse und vermeintliche Verstösse dem EDÖB melden, um sich selber zu entlasten. Die vorgeschlagene Sanktionslösung führt darüber hinaus bei schweizerischen Unternehmen zu Wettbewerbsnachteilen, da die Vollstreckung allfälliger Sanktionen gegenüber ausländischen Unternehmen stark erschwert sein dürfte. Des Weiteren verstösst die vorgeschlagene Regelung gegen gewichtige (rechtsstaatliche) strafprozessuale Prinzipien und könnte daher im Ergebnis zu Vollstreckungsproblemen führen. Aufgrund der teilweise sehr unklaren oder unbestimmten Regelung der strafbedrohten Pflichten ist das strafrechtliche Bestimmtheitsgebot tangiert. Es ist z.B. betreffend die Pflichten in Art. 18 VE-DSG vollkommen unklar, welche Massnahmen unter diesem Gesichtspunkt implementiert werden müssen. Weder die Datenbearbeiter, noch der Strafrichter können aufgrund dieser gesetzlichen Regelung beurteilen, ob die besagten Pflichten eingehalten sind oder nicht. Tangiert ist aufgrund der verschiedenen Informations-, Melde- und Mitwirkungspflichten im VE-DSG auch der Grundsatz „nemo tenetur“, d.h. das Selbstbelastungsgebot. Die Pflicht,

					Datenschutzverstösse zu melden, welche ihrerseits strafbedroht ist, führt faktisch zu einer Selbstanzeigepflicht. Betreffend die Ausgestaltung eines alternativen Sanktionssystems verweisen wir auf den entsprechenden Vorschlag der economiesuisse. Im Vordergrund sollen Verwaltungsstrafen gegen das Unternehmen und nicht die natürlichen Personen stehen. Anknüpfungspunkt für die Strafbarkeit der Unternehmen sollen, wie in Art. 102 StGB, Organisationsmängel im Unternehmen sein, d.h. eine mangelhafte Datenschutz-Compliance. Lediglich subsidiär soll eine Strafbarkeit von Mitarbeitern möglich sein, wenn diese absichtlich bzw. mit Vorsatz gegen interne oder gesetzliche Datenschutzregeln verstossen haben. Eine Abstimmung hat hierbei mit bestehenden Bestimmungen im besonderen Teil des Strafgesetzbuches zu erfolgen (Geheimnisschutz, unbefugte Datenbeschaffung, etc.). Anzeigen sollen in dieser Konstellation primär durch die Unternehmen selbst erfolgen. Zuletzt ist der Kreis der potenziell strafrechtlich bedrohten Mitarbeiter einzuschränken. Um ein rechtsstaatlich korrektes Sanktionssystem zu erzielen, darf nicht der EDÖB über die Verwaltungssanktionen entscheiden. Wie im allgemeinen Strafprozessrecht darf die untersuchende bzw. anklagende Behörde nicht gleichzeitig die urteilende Behörde sein. Es muss daher eine neue urteilende Behörde für das Datenschutzrecht geschaffen werden. Das Verhältnis zwischen dieser neuen Behörde und dem EDÖB wäre im DSG zu regeln. Betreffend die Anpassung des Strafkataloges in Art. 50 und 51 VE-DSG wird auf die detaillierten Aufführungen in der Stellungnahme von economiesuisse verwiesen. Kbdirect unterstützt die entsprechenden Vorschläge.
kbdirect	DSG	52			**Kbdirect lehnt den neu vorgeschlagenen Art. 52 VE-DSG strikte ab. Es handelt sich um eine überschiessende Regelung, welche weder durch den E-SEV 108 noch die EU-DSGVO vorgesehen sind**. Art. 52 VE-DSG widerspricht auch dem allgemeinen Mechanismus des schweizerischen

					Datenschutzrechts. Nach dem geltenden DSG und auch nach den Bearbeitungsgrundsätzen im VE-DSG dürfen „normale“ Personendaten grundsätzlich ohne einen Rechtfertigungsgrund an Dritte weitergegeben werden – sofern auch die anderen Datenbearbeitungsgrundsätze eingehalten wurden. Nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile wurde im geltenden DSG vermutet, dass die Bekanntgabe an Dritte ohne Zustimmung der betroffenen Person eine Persönlichkeitsrechtsverletzung darstellt. Art. 52 VE-DSG würde diesem Konzept widersprechen. Obwohl der materielle Teil des Datenschutzgesetzes für die Bekanntgabe von normalen Personendaten an Dritte keinen Rechtfertigungsgrund verlangt, könnte diese an sich zulässige Bekanntgabe wegen Art. 52 VE-DSG dennoch strafbar sein. **Die Problematik wird dadurch verschärft, dass der Begriff „geheim“ unklar ist. Die Ausführungen im erläuternden Bericht erhöhen die Unklarheiten bzw. legen eine sehr extensive Auslegung des Geheimnisbegriffes nahe.**

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
kbdirect	3 lit. a	Die Ausführungen zum Begriff der Personendaten sind widersprüchlich bzw. sorgen für Rechtsunsicherheit. Es wird einerseits ausgeführt, dass keine Änderungen an der geltenden Begriffsbestimmung beabsichtigt wird, danach wird jedoch unnötig aus den Erwägungsgründen der EU-DSGVO zitiert, nota bene aus Erwägungsgründen, welche bereits in der EU für Unklarheiten sorgten. Es reicht aus, wenn in den Materialien auf die geltende Praxis und Rechtsprechung verwiesen wird. Zudem soll klargestellt werden, dass für die Bestimmbarkeit die sog. relative Methode relevant ist.
kbdirect	3 lit. f	Die Ausführungen zum Profiling sind nicht hilfreich und führen im Vergleich zum vorgeschlagenen Gesetzeswortlaut nicht zu einer Präzisierung. Der Begriff des Profiling muss in den Materialien genauer konkretisiert werden. Wichtig ist zudem, dass der Begriff auf

		automatisiertes Profiling eingeschränkt wird. Dies entspricht auch der Lösung in der EU. Des Weiteren ist klarzustellen, dass nicht jede automatisierte Auswertung zwingend zu einer Beeinträchtigung der Persönlichkeit führen muss. Profiling im Sinne des Gesetzes ist auf Auswertungen zu beschränken, welche zu einer erheblichen Beeinträchtigung der Persönlichkeit führen.
kbdirect	4 Abs. 6	**Es wird zwar ausgeführt, dass es sich nur um eine terminologische Annäherung an die EU-DSGVO handelt, doch werden die strengen Anforderungen an die Einwilligung in der EU-DSGVO gerade aus dem Wortlaut abgeleitet.** In den Materialien ist daher klarzustellen, dass gegenüber den Anforderungen an die Einwilligung nach geltendem DSG keine Änderung beabsichtigt wird. Insbesondere werden die strengen Anforderungen aus der EU-DSGVO klar nicht übernommen. Es muss auch nach zukünftigem DSG möglich sein, die Einwilligung im Rahmen von AGB einzuholen und zwar nicht separat oder getrennt von anderen Informationen. Auch Stillschweigen muss unter gewissen Umständen als Einwilligung gelten.
kbdirect	8	Die Materialien müssen klarstellen, dass die Initiative für solche Empfehlungen von den Branchenverbänden ausgehen muss. Der EDÖB soll kein Recht haben, selber Empfehlungen zu erlassen. Gegen die Genehmigung oder Nicht-Genehmigung von Empfehlungen (durch den EDÖB) muss es sodann Rechtsmittel geben. In den Materialien sind die wichtigsten Voraussetzungen betreffend diese Rechtsmittel zu erläutern (z.B. Legitimation, etc.).
kbdirect	13	In den Materialien sind die Einzelheiten, insbesondere auch betreffend die Umsetzung der Informationspflicht, genauer festzulegen. Es ist klarzustellen, dass die Information in allgemeiner Form in einer Datenschutzerklärung auf der Webseite erfolgen kann. Dies ist auch durch die E-SEV 108 vorgesehen. Der Hinweis im erläuternden Bericht, dass die betroffene Person nicht nach den Informationen suchen muss, ist dahingehend einzuschränken, dass bei einer Datenschutzerklärung auf der Webseite diese Voraussetzung erfüllt ist. In den Materialien ist zudem explizit klarzustellen, dass die Informationspflicht sich auf den Zeitpunkt der Datenbeschaffung beschränkt. Eine Nachinformation ist nicht notwendig. Dies entspricht auch dem vorgeschlagenen Gesetzeswortlaut („spätestens bei der Datenbeschaffung“). Sofern an der Informationspflicht bei der indirekten Datenbeschaffung festgehalten wird, ist in den Materialien auch klarzustellen, wie die Information erfolgen muss. Damit hier keine unnötigen Umsetzungsschwierigkeiten entstehen und auch im Sinne des risiko-basierten Ansatzes muss es auch hier möglich sein, die Information mittels Datenschutzerklärung auf der Webseite sicherzustellen. Zudem muss den Unternehmen für die Information bei der indirekten Datenbeschaffung mehr Zeit eingeräumt werden. Entgegen dem vorgeschlagenen Wortlaut in der VE-DSG erlauben sowohl die E-SEV-108 als auch die EU-DSGVO bei der Information eine

		zeitliche Verzögerung.
kbdirect	15	Es ist klarzustellen, dass auch „rechtliche Auswirkungen" eine gewisse Schwere aufweisen müssen. Sonst ist diese Informationspflicht überschiessend und führt zu hohem administrativem Aufwand, ohne den Schutz der betroffenen Personen effektiv zu verbessern.
kbdirect	18	Die Ausführungen zu diesen beiden Pflichten ist unklar. In den Materialien ist zu betonen, dass bei der Frage der Umsetzung dieser Pflichten der risikobasierte Ansatz entscheidend ist. Dies führt dazu, dass Privacy by Design z.B. nicht bei jeder Datenbearbeitung massgeblich ist. Die Datenbearbeiter müssen einen gewissen Spielraum haben und die Anstrengungen auf Datenbearbeitungen mit höherem Risiko fokussieren.
kbdirect	23 Abs. 3	Der Hinweis darauf, dass dieser Rechtfertigungsgrund nur dann erfüllt ist, wenn die Datenbearbeitung rechtmässig erfolgt, ist in den Materialien zu streichen. Es genügt ein Verweis auf die bestehende Praxis zum geltenden DSG.
kbdirect	24 Abs. 2	Entsprechend der EU-DSGVO (Erw.-Gr. 47) ist in den Materialien explizit darauf hinzuweisen, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
kbdirect	50 ff.	**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt**. Das vorgeschlagene Sanktionssystem ist in höchstem Masse innovationshemmend und führt zu einem ganz erheblichen Standortnachteil der Schweiz. Kein innovatives digitales Start-Up wird bereit sein, seine Gründer und Mitarbeiter solch drastischen strafrechtlichen Risiken auszusetzen. Gute Mitarbeiter werden nicht mehr bereit sein, Verantwortung in den Unternehmen mitzutragen. Kbdirect schliesst sich, wie bereits vorangehend bei den Bemerkungen zu den einzelnen vorgeschlagenen Bestimmungen ausgeführt, der Forderung von economiesuisse nach einem alternativen, datenschutzgerechten Sanktionssystem an. Dieses alternative Sanktionssystem soll primär auf Verwaltungssanktionen abstellen, welche sich gegen die Unternehmen selbst richten. Nur ausnahmsweise, bei direktem Vorsatz oder Absicht, soll eine subsidiäre Strafbarkeit von natürlichen Personen greifen.
kbdirect	Seite 88	**Es ist eine angemessene Übergangsfrist von mindestens zwei Jahren für die Umsetzung aller neuen Pflichten vorzusehen.** Der Umsetzungsaufwand darf nicht unterschätzt werden. Eine Umsetzungsfrist von zwei Jahren stimmt auch mit der

		entsprechenden Regelung in der EU-DSGVO überein. Darüber hinaus ist in den Materialien klarzustellen, dass die neuen Bestimmungen keine Rückwirkung haben. Personendaten, welche vor dem Inkrafttreten der neuen Bestimmungen rechtmässig beschafft wurden, gelten weiterhin als rechtmässig beschafft. War z.B. nach geltendem Recht für eine bestimmte Datenbeschaffung und – bearbeitung keine ausdrückliche Information oder gar eine Zustimmung notwendig, dürfen diese Daten auch zukünftig ohne Nachinformation oder Nacheinwilligung bearbeitet werden, sofern sich an der Bearbeitung dieser Personendaten (z.B. am Bearbeitungszweck) nichts ändert.

Amstutz Jonas BJ

Von: Muffler, Roger <R.Muffler@kbdirect.ch>
Gesendet: Freitag, 31. März 2017 16:30
An: Amstutz Jonas BJ
Betreff: Stellungnahme der KünzlerBachmann Directmarketing AG zum VE-DSG
Anlagen: Vernehmlassung_VE-DSG_kbdirect_31032017.doc

Sehr geehrter Herr Amstutz

Gerne bringen wir uns in die laufende Vernehmlassung zum VE-DSG ein und senden Ihnen im Anhang unsere Stellungnahme.

Dürfte ich Sie um eine kurze Eingangsbestätigung bitten?

Bei Rückfragen stehe ich selbstverständlich gerne zur Verfügung.

Besten Dank im Voraus für Ihre Bemühungen

Herzliche Grüsse

Roger Muffler
Head of Data / Member of Management

künzlerbachmann
directmarketing

KünzlerBachmann Directmarketing AG
Zürcherstrasse 601 . CH 9015 St.Gallen
T +41 71 314 04 21 . F +41 71 314 04 05
r.muffler@kbdirect.ch . www.kbdirect.ch

Amstutz Jonas BJ

Von: Jan Ramseyer <j.ramseyer@konsum.ch>
Gesendet: Dienstag, 4. April 2017 10:28
An: Amstutz Jonas BJ
Cc: Babette Sigg Frank
Betreff: Stellungnahme Totalrevision DSG
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de_kf.doc

Sehr geehrter Herr Amstutz

Im Anhang lasse ich Ihnen die Stellungnahme des Schweizerischen Konsumentenforum kf zur Revision des DSG zukommen.
Wir haben versucht, die Stellungnahme möglichst aus der Konsumentensicht zu formulieren. Zudem haben wir uns eher allgemein gehalten.

Mit freundlichen Grüssen
Jan Ramseyer

--
Jan Ramseyer
Projektleiter / Projektkoordination

Konsumentenforum kf
Belpstr. 11, 3007 Bern
Tel. 031 380 50 32
www.konsum.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerisches Konsumentenforum kf

Abkürzung der Firma / Organisation : kf

Adresse : Belpstrasse 1, 3007 Bern

Kontaktperson : Jan Ramseyer

Telefon : 031‘380‘50‘32

E-Mail : j.ramseyer@konsum.ch

Datum : 04.01.2017

Wichtige Hinweise:

1. Wir bitten Sie, keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.kf	Sehr geehrte Damen und Herren Wir danken Ihnen für die Gelegenheit, zur Vorlage „Bundesgesetz über die Revisionen des Bundesgesetzes über den Datenschutz (DSG)“ Stellung nehmen zu dürfen, und stellen Ihnen nachfolgend unsere Anliegen zu. Vorausschicken möchten wir, dass die Stellungnahme eher allgemein gehalten ist. Das Schweizerische Konsumentenforum kf anerkennt und begrüsst die Revision des Datenschutzgesetzes (VE-DSG). Mit der fortschreitenden Digitalisierung nimmt die Bedeutung von Daten zu. Sie bilden die Grundlage für neue Geschäftsfelder, Dienstleistungen und Anwendungen. Ein modernes, griffiges und praxisnahes Datenschutzgesetz ist unter den sich ständig verändernden gesellschaftlichen und technischen Verhältnissen unabdingbar. Das kf unterstützt die angestrebte Verbesserung der Transparenz bei der Datenbearbeitung. Naheliegend ist dabei, dass ein optimales Verhältnis zwischen dem Nutzen für die betroffenen Personen und der Praktikabilität für Unternehmen (Verantwortliche oder Auftragsbearbeiter) zu finden ist. Aus der Sicht des Konsumentenforums muss bei den Betroffenen neben der Transparenz auch ein Bewusstsein für Daten sowie die Bedeutung und Auswirkung derer Verarbeitung geschaffen werden. In verschiedenen Paragraphen allerdings stellt das Konsumentenforum kf Ansätze eines «SWISS FINISH» fest, obwohl dieser gemäss Bericht Punkt 1.7.4 nicht angestrebt wird. Wir beurteilen dies eher kritisch. Die Schwierigkeit bei der Umsetzung des Gesetzes besteht in den Augen des kf in der Dynamik der Entwicklungen. Digitalbasierte Produkte entwickeln sich mit exponentieller Geschwindigkeit. Somit liegt der Schluss nahe, dass Gesetze im Bereich Datenschutz nur schwer aktuell zu halten sind. Die Artikel 8 bis 10 (VE-DSG) bieten die Möglichkeit zur Selbstregulierung. Diesem Teil des Gesetzes sollte noch mehr Bedeutung zukommen. Die Selbstregulierung ermöglicht ein schnelles und flexibles Reagieren auf neu auftretende Herausforderungen. Verschiedene Ombudsstellen sollten dabei gefördert werden. Sie können bei der Vermittlung zwischen Firmen und Konsumenten eine wichtige Rolle einnehmen. Weiter können sie auftretende Probleme mit Branchenvertretern besprechen und gemeinsam mit ihnen Lösungen erarbeiten. Vor dem Hintergrund des Entwicklungsausmasses im Bereich „Datenverarbeitung“ sieht das kf die dem Beauftragten (EDÖB) zugetragenen Aufgaben von diesem alleine (resp. der auszubauenden Stelle) als nicht erfüllbar. Es müssen wie erwähnt mehr andere Organe miteinbezogen werden. Dem Ausbau der Kompetenzen des EDÖB stehen wir kritisch gegenüber. In unseren Augen besteht die Gefahr, dass diese zu wenig weit geht.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Fehler! Verweisquelle konnte nicht gefunden werden.kf	**1) Konsumenten und Daten:** a) Das Schweizerische Konsumentenforum ist der Ansicht, dass es Schweizer Konsumentinnen und Konsumenten (in der Folge Konsumenten genannt) teilweise Mühe bereitet, die Zusammenhänge der Datenflüsse zu verstehen. Was geschieht mit meinen Daten, wer kann sie einsehen, wo sind sie gespeichert etc. All dies sind Fragen, die unbeantwortet oder vom Konsumenten oft unbeachtet bleiben. b) Die Menge an Daten, die Konsumenten generieren und damit einhergehend die Quantität an zu verarbeitenden Daten nehmen zu. Ein **risikobasierter Ansatz**, wonach umzusetzende Massnahmen sich nach der Höhe des Risikos zu orientieren haben, ist wünschenswert. Nach Ansicht des kf interessiert sich der Konsument nicht für sämtliche Stufen eines Datenstromes. Über „risikoreiche" Schritte oder Zustimmungen muss er allerdings aufgeklärt werden. Die **Informationspflicht** soll so ausgestaltet sein, dass die betroffene Person darüber informiert wird, wenn sensible Daten erhoben werden oder „schwerwiegende" Veränderungen, (genauer zu definieren) anstehen. So kann eine undifferenzierte Informationsflut bei den betroffenen Personen verhindert werden. Sie können über relevante Vorgänge einfacher und selbständig entscheiden. c) Die **AGB** eines Vertrages beinhalten oftmals auch die Bestimmungen zu Beschaffung und Verarbeitung von Personaldaten. Erfahrungsgemäss werden diese AGB von Konsumenten nicht immer in vollem Umfang studiert. Es gilt zu prüfen, ob neuralgische, entscheidungsrelevante Informationen bezüglich Datenerhebung und den Umgang mit Daten durch den Verantwortlichen in den AGB besonders hervorgehoben werden müssen. Denkbar: Der Konsument muss den fünf für ihn wichtigsten Punkten zusätzlich zu den AGB zustimmen. Diese sind einfach zu präsentieren und in wenigen Worten zu präzisieren (bei digitalen Verträgen ist dies technisch einfach umsetzbar). Diese Massnahme fördert zudem Datenbewusstsein und Datenverständnis des Konsumenten. Das Gesetz lässt grundsätzlich jedoch zu wenig Spielraum für solche Lösungen. Wir sind uns aber auch bewusst, dass Gesetzgebung und –umsetzung komplex sind.
Fehler! Verweisquelle konnte nicht gefunden werden.kf	2) **Unternehmungen und Daten** a) Der vorliegende Entwurf beachtet in den Augen des kf den Fakt zu wenig, dass damit in Zukunft sämtliche in der Schweiz tätige Unternehmen ,welche mit natürlichen Personen zu tun haben, mit erheblichen Mehraufwänden konfrontiert werden. Es stellt sich die Frage nach dem Nutzen für Konsumenten und Unternehmer. Das Konsumentenforum befürchtet eine Verkomplizierung der Geschäftsabwicklungen zwischen Konsument und Produzent durch zu strikte Auflagen. b) Das Gesetz tendiert dazu, Grossunternehmen, welche international tätig sind (Google, Facebook, Amazon etc.) zu bevorteilen. Nur in der Schweiz tätigen Unternehmen werden Hürden auferlegt, welche im schlechtesten Fall zu einem Wettbewerbsnachteil gegenüber international agierenden Unternehmen führen könnten.

Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.kf	DSG	2			Geltungsbereich generell: Nicht klar ist, wie genau juristische Personen betroffen sind. In Anbetracht von Art. 50 ff. VE-DSG ist dies unbedingt zu regeln. Es fehlt nach Ansicht des kf auch eine klare Bestimmung, welche besagt, dass das Datenschutzrecht für in der Schweiz wohnhafte / gemeldete Personen gilt. Es ist klarzustellen, dass bei einer Regelung jedes Unternehmen, unabhängig davon, wo es seinen Sitz hat, die Schweizer Datenschutzgesetze zu befolgen hat. Nur so bringt das Gesetz den Konsumenten den gewünschten Nutzen.
Fehler! Verweisquelle konnte nicht gefunden werden.kf	DSG	3	a		Der Begriff „bestimmbare Personen“ ist zu wenig klar. Eine Präzisierung ist wünschenswert.
Fehler! Verweisquelle konnte nicht gefunden werden.kf	DSG	16			Pflicht zur vorgängigen Datenschutz-Folgeabschätzung: Diese Vorschrift ist in den Augen des kf nicht haltbar. Einerseits werden inländische Firmen daran gehindert, Innovationen schnell an ihre Kundschaft zu bringen. Andererseits ist es Schweizer Konsumenten möglich, digitalisierte Produkte aus dem Ausland zu beziehen. Sollten ausländische Firmen ihre digitalen Produkte erst vom Verantwortlichen prüfen lassen, bevor sie verkauft werden dürfen, fördert dies einerseits Graumärkte, anderseits werden Schweizer Konsumenten benachteiligt. Weisen Firmen von sich aus auf Risiken hin (vgl. Konsumenten und AGB), sollte sich der Konsument des Risikos bewusst sein, die bei der Benützung eines Dienstes oder Produktes entsteht. Es sind Regelungen zu schaffen, welche die Selbstregulierung und Selbstverantwortung der Konsumenten fördern und ermöglichen.

Fehler! Verweisquelle konnte nicht gefunden werden.kf	DSG	50	ff		Das Konsumentenforum fordert eine Strafbestimmung, die klar zwischen Unternehmen und Privatpersonen unterscheidet
Fehler! Verweisquelle konnte nicht gefunden werden.kf	DSG	27	ff		Aus der Sicht des Konsumentenforums ist hier der Unterschied zwischen Firmen und Bundesorganen teils nicht plausibel. Folgend zwei Beispiele, die das kf dazu veranlassen, eine Überarbeitung der Artikel zu fordern.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	27	3	b	Dürften hier Firmen Daten ebenfalls bearbeiten oder gar speichern, falls die Person diese öffentlich macht, ohne die Person über den Zweck zu informieren?
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	29			An wen dürfen diese bekannt gegeben werden? Dürfen Firmen diese nicht schützenswerten Daten ebenfalls bearbeiten oder speichern?
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden		

werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Barbara Zinggeler <barbara.zinggeler@kka-ccm.ch>
Gesendet: Montag, 3. April 2017 15:24
An: Amstutz Jonas BJ
Cc: Barbara Zinggeler
Betreff: DSG: Stellungnahme KKA-CCM
Anlagen: Totalrevision-Datenschutzgesetz_Formular-Stellungnahme_KKA_def_17_04_03.doc

Wichtigkeit: Hoch

Bundesgesetz über die Totalrevision des Datenschutzgesetztes (Vorentwurf): Stellungnahme der Konferenz der Kantonalen Ärztegesellschaften KKA-CCM

Sehr geehrter Herr Amstutz

Anbei erhalten Sie fristgerecht und wie gewünscht im word-Format unsere Stellungnahme zu dieser Gesetzesvorlage, welche die Interessenwahrung der Ärzteschaft und die ihrer Patienten in verschiedenen Punkten stark tangiert.

Wir danken Ihnen für den Einbezug unserer Überlegungen und Argumente und grüssen Sie freundlich

Barbara Zinggeler

KKA CCM CMC

Konferenz der Kantonalen Ärztegesellschaften
Barbara Zinggeler lic.phil., Geschäftsführerin
Nordstrasse 15, CH-8006 Zürich
Tel. +41 (044) 421 14 44 Fax: +41 (0)44 044 421 14 15
barbara.zinggeler@kka-ccm.ch www.kka-ccm.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Konferenz der kantonalen Ärztegesellschaften

Abkürzung der Firma / Organisation : KKA

Adresse : Geschäftsstelle KKA-CCM, Nordstrasse 15, 8006 Zürich

Kontaktpersonen : Frau lic. phil. Barbara Zinggeler / Prof. Dr. iur. Urs Saxer

Telefon : 044 421 14 44 / 044 269 4000

E-Mail : barbara.zinggeler@kka-ccm.ch / saxer@steinlex.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	Die KKA als Verbund von nahezu allen kantonalen Ärztegesellschaften vertritt die Interessen der freipraktizierenden Ärztinnen und Ärzte in der Schweiz. Als Standesorganisation setzt sie sich nicht nur für die Interessen der den kantonalen Gesellschaften angeschlossenen Ärztinnen und Ärzte ein, sondern auch für ein gut funktionierendes, erschwingliches und qualitativ hochstehendes Gesundheitswesen. Dazu trägt die in freier Praxis tätige Ärzteschaft ganz entscheidend bei. Ärztinnen und Ärzte mit eigener Praxis oder als Mitarbeitende von Gemeinschaftspraxen sind für die breite Bevölkerung die primären Ansprechpartner in Gesundheitsfragen. Sie sind für Patientinnen und Patienten Vertrauenspersonen. Letztere offenbaren dem behandelnden Ärztinnen und Ärzte wichtige Informationen über die eigene Person und die eigene Gesundheit. Zugleich gelangen ärztliche Fachpersonen als Teil ihrer Tätigkeit, z. B. im Rahmen der Anamnese und der Diagnose, zu wesentlichen Informationen über den physischen oder psychischen Gesundheitszustand einer Person. Es ist daher offensichtlich, dass datenschutzrechtliche Problemstellungen im Zusammenhang mit der ärztlichen Tätigkeit eine ganz zentrale Bedeutung einnehmen. Die Ärzteschaft ist sich dessen bewusst. Das Arztgeheimnis ist ein zentrales Instrument, um die Interessen der Patientinnen und Patienten an der Vertraulichkeit von Informationen über die eigene Person zu schützen. Die Verpflichtungen der Ärzteschaft, das Arztgeheimnis zu schützen und zu achten ist unabdingbarer Bestandteil einer erfolgreichen und vertrauensbasierten ärztlichen Tätigkeit. Es ist nun allerdings nicht zu übersehen, dass das Arztgeheimnis und damit auch der Schutz der Privat- und Intimsphäre der Patientinnen und Patienten stark gegenläufigen Tendenzen ausgesetzt ist. Hierfür gibt es mehrere Gründe. Der technisch medizinische Fortschritt und die immer ausgeprägtere Spezialisierung innerhalb der Ärzteschaft verlangt immer stärker einen Austausch von Daten innerhalb der ambulant tätigen Ärzteschaft, aber auch zwischen Ärzten und Spitälern, Apotheken etc. Je integrierter die Gesundheitsversorgung ist, desto wichtiger wird der Austausch von Patientendaten, welche zum Teil sensibler Natur sind. Eine weitere Herausforderung für den Datenschutz im Gesundheitswesen ist finanziell bedingt. Die Versicherer verlangen im Rahmen der Wirtschaftlichkeitsprüfungen zunehmend detaillierte Angaben über ärztliche Behandlungen von bestimmten Patienten. Diesem Datenhunger der Versicherer kommt der Datenhunger der öffentlichen Hand durchaus gleich. Art. 30 ff. KVV verlangt von den Leistungserbringern, und damit auch von den freipraktizierenden Ärztinnen und Ärzte die Bekanntgabe wesentlicher Daten über die eigene Tätigkeit. Was die Patientendaten anbelangt, so erfolgt die Weitergabe auf anonymisierter Basis. Demgegenüber sind die Ärztinnen und Ärzte verpflichtet, gegenüber dem Bundesamt für

	Statistik wesentliche Angaben über die eigene Geschäftstätigkeit offen zu legen. In soweit gibt es für die freipraktizierende Ärzteschaft gegenüber dem Staat keinen Datenschutz. Das Beispiel zeigt, dass Datenschutzfragen im Gesundheitswesen nicht nur aus der Patientenperspektive zu beleuchten sind, sondern auch aus der Perspektive der Leistungserbringer und deren Rechte sowie Pflichten. Schliesslicht ist zu bemerken, dass die freipraktizierende Ärzteschaft aus Gründen der Effizienz sowie der Konzentration auf die Kerntätigkeit immer stärker einzelne administrative Tätigkeiten ausgelagert hat, so insbesondere das Rechnungswesen. Auch dies führt dazu, dass Daten der Arztpraxen, aber auch von einzelnen Patienten von Dritten bearbeitet werden. Die Dokumentation und Informationspflichten der freipraktizierenden Ärzteschaft sind in den letzten Jahren ganz erheblich erweitert worden. Dies führt dazu, dass die Belastung der Ärzteschaft durch diese Art der Tätigkeit finanziell und zeitlich erheblich zugenommen hat. Es gibt angesichts dessen auch eine Grenze der Zumutbarkeit, was den Aufwand in administrativer Hinsicht anbelangt. Dazu gehören auch datenschutzrechtliche Aspekte. Die KKA begrüsst die allgemeine Stossrichtung des nunmehr präsentierten Vorentwurfs. Unbestritten sind als Grundanliegen: Die möglichst weitgehende, wenn auch nicht zwingend vollständige Harmonisierung der schweizerischen Datenschutzgesetzgebung mit den europäischen Vorgaben, die Verbesserung des Datenschutzes natürlicher Personen in ausgewählten Aspekten. Verschiedenste Aspekte des Gesetzes sind positiv zu würdigen, wie nachfolgend bei der Kommentierung einzelner Bestimmungen des Vorentwurfes aufgezeigt werden wird. Es gibt allerdings auch Aspekte, welche für die freipraktizierende Ärzteschaft weniger vorteilhaft sind. Dazu zählen nebst einigen Unklarheiten mit Bezug auf die möglichen Auswirkungen auf die freipraktizierende Ärzteschaft vor allem die Befürchtung einer weiteren Zunahme der administrativen Belastung und die erhebliche Verschärfung sowie Erweiterung des Strafrahmens. Dies ändert allerdings nichts daran, dass die KKA dem Vorhaben einer Totalrevision des DSG grundsätzlich positiv gegenübersteht. Nach bald 25 Jahren macht es zweifelsohne Sinn, den Datenschutz den geänderten Verhältnissen anzupassen. Zentral für die KKA ist in diesem Zusammenhang, dass gesetzliche Regelungen gebildet werden, welche eine Berücksichtigung der Besonderheiten im Gesundheitsbereich und insbesondere der Tätigkeit der freipraktizierenden Ärzteschaft zulassen.
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler!	

Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
KKA	DSG	1			Das neue Gesetz schliesst den Schutz der Persönlichkeit und der Grundrechte von juristischen Personen nicht mehr in den Gesetzeszweck ein. In der Tat unterschied sich diesbezüglich, mit dem stark erweiterten, auch auf juristische Personen bezogenen Schutzbereich die schweizerische Gesetzgebung von den vergleichbaren Rechtsnormen in der EU sowie in anderen Staaten. Aus Sicht der KKA ist entscheidend, dass weiterhin auch dann die Daten natürlicher Personen geschützt sind, wenn diese im Besitze juristischer Personen sind und von diesen bearbeitet werden. Was die Ärzteschaft als Leistungserbringer anbelangt, so sind auch frei praktizierende Ärztinnen und Ärzte, welche Einzelfirmen sind, weiterhin vom Gesetz geschützt. Dies ist demgegenüber offensichtlich nicht mehr der Fall bei als juristische Körperschaften organisierten Leistungserbringern. Dies ist wohl notgedrungen in Kauf zu nehmen.
KKA	DSG	2			Art. 2 bestimmt den Geltungsbereich des Gesetzes. Es ist klar und auch völlig richtig, dass ärztliche Leistungserbringer, d. h. also Ärztinnen und Ärzte sowie als juristische Personen organisierte ärztliche Leistungserbringer Patientendaten bearbeiten und daher vom Gesetz erfasst werden. Problematisch ist indessen, dass das Gesetz keinerlei Regelungen trifft, was das Verhältnis zu anderen Gesetzen anbelangt. Im Gesundheitsbereich kann dies ein ernsthaftes Problem sein. Die Abgrenzungen sind bei weitem nicht eindeutig. Das Bundesgesetz über das elektronische Patientendossier EPDG und das KVG enthalten wichtige, auch datenschutzrechtlich relevante Bestimmungen. Im welchem Verhältnis stehen diese Normen zum neuen DSG? Die Fragestellung ist alles andere denn banal. Denn gemäss dem Gesetzesentwurf sind die Sanktionen schärfer als unter dem geltenden Recht. Es ist daher für die ärztlichen Leistungserbringer von erheblicher Bedeutung zu wissen, ob die speziellen Regelungen in den genannten Gesetzen vorgehen, im Übrigen aber die Bestimmungen des DSG gelten, oder ob mit den Regelungen in den Spezialgesetzen die Geltung des DSG generell ausgeschlossen wird. Aus Sicht der Ärzteschaft ist eine entsprechende Klärung mehr als wünschbar. Dies muss nicht zwingend in Art. 2 geschehen. Die derzeitige Gesetzesvorlage spricht sich indessen generell zu diesem zentralen Problem nicht aus. Aus Sicht der Ärzteschaft stellt dies eine wesentliche, mit grossen Rechtsunsicherheiten

					verbundene Unterlassung dar.
KKA	DSG	3			Was die grundsätzlich sehr wünschbaren Definitionen in Art. 3 anbelangt, so sind aus Sicht der ambulant tätigen Ärzteschaft vor allem die Bestimmungen zu den besonders schützenswerten Personendaten sowie zum Profiling relevant. Es bedarf keiner näheren Erläuterung, dass Daten über die Gesundheit besonders schützenswert sind. Es ist auch klar, dass diese Qualifikationen zu erhöhten Sorgfaltspflichten führt, welche im Gesetz näher ausgeführt sind. Was das Profiling anbelangt, so sei der Hinweis erlaubt, dass die ärztliche Tätigkeit häufig, wenn nicht zumeist auch in einem Profiling bezüglich des Gesundheitszustandes besteht. Mit anderen Worten: Ärztinnen und Ärzte müssen sich an die Regelungen halten, welche im Gesetz sich auf das Profiling beziehen, insbesondere an die damit verbundenen erhöhten Sorgfaltspflichten. Nun ist eigentlich das Profiling auf andere Konstellationen bezogen: Nämlich auf das Sammeln und Verbinden von Daten über eine Person ohne deren Einwilligung, um von dieser Person ein Profi zu gewinnen. Diese Konstellation unterscheidet sich erheblich vom Profiling im Rahmen des Gesundheitswesens bzw. von ambulant tätigen Ärztinnen und Ärzten. Denn dort findet das Profiling freiwillig und mit der ausdrücklichen oder zumindest konkludenten Zustimmung der Patientinnen und Patienten statt. Es stellt sich daher ganz ernsthaft die Frage, ob sich eine Anwendung der strengeren Bestimmungen zum Profiling auf die Ärzteschaft rechtfertigt. Zu denken ist z. B. an das Profiling in Notfällen oder bei psychischen Erkrankungen. Dies gilt im Übrigen auch für die Umschreibung des Begriffes des Verantwortlichen bzw. des Auftragsbearbeiters. Sind ärztliche Leistungserbringer, ist der in freier Praxis tätige Arzt Verantwortlicher im Sinne von Art. 3 lit. h DSG? Es ist wohl davon auszugehen. Jede Krankheitsgeschichte stellt eine Bearbeitung in einer Art und Weise dar, dass der Bearbeitende ein Verantwortlicher ist. Ist dies im Gesundheitsbereich wirklich sachgerecht?
KKA	DSG	4			Aus Sicht der KKA ist gegen die allgemeinen Bestimmungen bzw. gegen die allgemeinen Grundsätze grundsätzlich nichts einzuwenden. Allerdings ist auf Probleme hinzuweisen, welche sich aus einer Anwendung von Art. 4 Abs. 6 im Arzt – Patientenverhältnis ergeben können. Nach dieser Bestimmung ist die ausdrückliche Einwilligung einer Person bei besonders schützenswerten Personendaten und beim Profiling erforderlich. Mithin bestehen erhöhte Anforderungen an das Einverständnis. Im Grundsatz ist

					dagegen nichts einzuwenden. Indessen stösst dies an Grenzen. Wie steht es in Notfällen oder bei psychischen Erkrankungen, welche die Urteils- und Handlungsfähigkeit einer Person in Frage stellen? In welchem Verhältnis steht die Regelung von Art. 4 Abs. 6 zu den Regelungen im EPDG? Was geschieht, wenn eine Patientin, wenn ein Patient diese Einwilligung verweigert, und es dadurch für die Ärztin oder den Arzt schwierig wird, die Anamnese vorzunehmen und eine geeignete Heilmethode vorzuschlagen? Wie sieht dies mit der Haftung des Arztes bzw. der Ärztin aus? Resultiert aus der fehlenden Einwilligung von Patientinnen und Patienten ein Selbstverschulden? Daraus ergibt sich, dass erhebliche, wichtige und nicht wenige Fragen offen sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	5			Keine Bemerkungen
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	6			Diese Bestimmung kann vor allem relevant sein bei Notfällen im Ausland. In einem solchen Fall kann unter Umständen die betroffene Person nicht einwilligen. Trotzdem kann es zum Schutz ihrer Gesundheit unabdingbar sein, dass Gesundheitsdaten in ein Land transferiert werden, das nicht dasselbe Schutzniveau hat wie die Schweiz. Art. 6 Abs. 1 Bst. d sieht völlig zu Recht die Möglichkeit vor, dass Personendaten ins Ausland bekannt gegeben werden können, wenn das Leben oder die körperliche Unversehrtheit bei der betroffenen Person in Frage steht. Es ist davon auszugehen, dass es immer auch dann der Fall ist, wenn ein Gesundheitsproblem vorliegt. Völlig unnötig ist aus Sicht der ambulant tätigen Ärzteschaft demgegenüber, dass in solchen Fällen der Beauftragte informiert werden muss. Nach Ansicht der KKA handelt es sich hier um einen Fall, bei welchem Empfehlungen der guten Praxis durch die Branche selber auszuarbeiten sind. Wie sich aus dem Kommentar zu Art. 8 DSG ergibt, ist die KKA der Auffassung, dass derartige Empfehlungen der guten Praxis unter gesetzlich definierten Umständen auch von den allgemeinen gesetzlichen Regelungen abweichen können (vgl. nachfolgend zu Art. 8), wenn sie vom Beauftragten genehmigt worden sind.
Fehler! Verweisquelle konnte nicht	DSG	7			Diese Bestimmung ist im Gesundheitsbereich von erheblicher Bedeutung, werden doch oft Patientendaten im Auftrag von Leistungserbringer oder aufgrund einer gesetzlichen Anordnung von Dritten bearbeitet. Was

gefunden werden.					die ambulant tätige Ärzteschaft anbelangt, so ist insbesondere die Rechnungsstellung und der Inkasso durch Unternehmungen wie z. B. die Ärztekasse zu erwähnen. Im Gesundheitsbereich wirft die an sich sinnvolle Bestimmung zwei Fragen auf, die unklar bleiben: Gemäss Art. 7 Abs. 1 gilt diese Bestimmung auch für den Fall einer Übertragung der Bearbeitung von Personendaten gestützt auf ein Gesetz. Wie ist dies zu verstehen? Bedeutet dies, dass überall dort, wo das Gesetz von Leistungserbringern verlangt (insbesondere das KVG), Daten zu liefern, Art. 7 zur Anwendung gelangt? Z. B. im Geltungsbereich des EPDG? Der KKA scheint diese Bestimmung in soweit unklar zu sein. Art. 7 Abs. 1 Bst. b) spricht gesetzliche Geheimhaltungspflichten an. Dazu gehört selbstverständlich auch das Arztgeheimnis. Bedeutet dies, dass eigentlich die Auftragsdatenbearbeitung für Leistungserbringer im Gesundheitswesen, insbesondere für ambulant tätige Ärztinnen und Ärzte unzulässig ist? Eine solche Auffassung würde auf jeden Fall völlig den Gepflogenheiten widersprechen. Zur Klärung der Verhältnisse wäre es zu begrüssen, wenn Art. 7 Abs. 1 eine Ziffer c. angefügt würde, welche wie folgt lauten kann: "Wenn die betroffene Person der Bearbeitung ihrer Personendaten durch einen Auftragsbearbeiter zustimmt." Diese Präzisierung würde wohl erheblich mehr Klarheit bringen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	8			Art. 8 ist eine interessante, grundsätzlich begrüssenswerte Bestimmung. Dies gilt insbesondere für das dort vorgesehene Konzept der regulierten Selbstregulierung. Grundsätzlich ist es zu begrüssen, wenn der Beauftragte auf dem Wege der Empfehlung Datenschutzvorschriften konkretisieren kann. Die Rechtsnatur dieser Empfehlung ist aber teilweise nicht klar. Mit Recht wird zwar in Art. 9 Abs. 2 darauf hingewiesen, dass die Datenschutzvorschriften auch auf andere Weise eingehalten werden können, als in Empfehlungen der guten Praxis vorgesehen ist. Die Empfehlungen sind mithin nicht umfassend rechtsverbindlich. Mit ihrer Einhaltung ist indessen klar, dass auch die Datenschutzvorschriften eingehalten werden. Insoweit ist trotz allem von einer limitierten Rechtsverbindlichkeit auszugehen. Dies bedeutet, dass Art. 8 praktisch eine Delegation von Rechtsetzungsbefugnissen an den Beauftragten enthält. Angesichts dessen wäre es wünschbar, wenn konkretisiert würde, unter welchen Voraussetzungen der Beauftragte Empfehlungen der guten Praxis erlassen soll. Denn es ist wohl davon auszugehen, dass die Verwaltungs- und Gerichtspraxis sich sehr

					stark an diesen Empfehlungen orientieren werden. Faktisch wird es so sein, dass in Bereichen, in denen eine Empfehlung besteht, deren Nichteinhaltung im Sine einer wiederlegbaren Vermutung eine Verletzung von Datenschutzvorschriften darstellt. Abs. 2 ist grundsätzlich inhaltlich zu begrüssen, aber nach Ansicht der KKA noch zu wenig konkret. So ist z. B. nicht klar, in welcher Form verantwortliche und interessierte Kreise die Empfehlungen des Beauftragten ergänzen können. Werden solche Ergänzungen ebenfalls gemäss Abs. 3 veröffentlich? Unklar ist sodann was unter "interessierte Kreise" zu verstehen ist. Im Gesundheitsbereich gibt es Akteure mit wiederstreitenden Interessen: die Leistungserbringer, die Versicherer, die Patienten und der Staat. Können sie alle je eigene Empfehlungen der guten Praxis erlassen? Wer prüft die Legitimation dieser "interessierten Kreise"? Wie legitimieren sich diese? Grundsätzlich ist sehr zu befürworten, wenn z. B. Branchenverbände eigene Empfehlungen der guten Praxis erarbeiten können. Diese Verbände verfügen über ein grosses know-how, denn ihre Arbeit ist von ausgeprägter Sachnähe geprägt. Indessen kann die Gefahr widersprechender Empfehlungen der guten Praxis nicht ausgeschlossen werden. Diese Gefahr kann nur durch eine Genehmigung der Empfehlungen durch den Beauftragten ausgeschlossen werden. Allerdings verlangt dies, wie nachfolgend zu zeigen sein wird, eine Präzisierung in Art. 9 Abs. 1. Was die Genehmigung anbelangt, so erfolgt diese durch den Beauftragten, falls die Empfehlungen eines Verantwortlichen oder interessierter Kreise mit dem Datenschutzvorschriften vereinbar sind. Es stellt sich allerdings die Frage, ob es nicht möglich sein sollte, unter gesetzlich umschriebenen Voraussetzungen und im Sinne einer Ausnahme auch Empfehlungen zu genehmigen, welche in nicht zentralen Bereichen der Datenschutzgesetzgebung von einzelnen Normen abweichen, weil der Gehalt der Empfehlung besser den Bedürfnissen und Gepflogenheiten einer Branche entspricht als die starren Regelungen des Datenschutzrechtes. Die KKA ist der Auffassung, dass dies näher zu prüfen ist. Gerade der Gesundheitsbereich weist z. B. sehr spezifische, auch widersprüchliche Bedürfnisse unter dem Gesichtswinkel des Datenschutzes auf. Es sollte z. B. möglich sein, in einzelnen Bereichen vom Erfordernis der ausdrücklichen Zustimmung, welches sonst bei besonders schützenswerten Daten gilt, abzuweichen. Hierfür könnte eine Empfehlung, genehmigt vom Beauftragten, genügen. Die Veröffentlichung von Genehmigungen ist zwingend erforderlich, führt doch deren Einhaltung dazu, dass die entsprechenden Datenschutzvorschriften eingehalten werden. Als in dem Sinne verbindliche

					Konkretisierung von einzelnen Bereichen der Datenschutzgesetzgebung muss eine Veröffentlichung erfolgen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	9			Vgl. hierzu auch die Bemerkungen zu Art. 8. Die Rechtsnatur der Empfehlungen ist unklar. Sie sind wohl am ehesten Verwaltungsverordnungen vergleichbar. Das Besondere daran ist, dass auch Empfehlungen privater bzw. "interessierter Kreise" im Fall der Genehmigung verbindliche Kraft haben können. Abs. 1 von Art. 9 hält nun allerdings ganz generell fest, dass ein Verantwortlicher die Datenschutzvorschriften einhält, wenn er die Empfehlung der guten Praxis befolgt, welche die entsprechenden Datenschutzvorschriften konkretisieren. Dies ist insoweit erstaunlich, als dass dies offensichtlich auch für nicht genehmigte Empfehlungen der guten Praxis interessierter Kreise, ja theoretisch sogar für Empfehlungen der guten Praxis Privater, welche der Beauftragte mangels Kompatibilität mit der Datenschutzgesetzgebung nicht genehmigt hat, gelten kann. Dies kann mit Sicherheit nicht die Meinung von Art. 9 Abs. 1 DSG sein. Die Bestimmung ist daher entsprechend zu ergänzen, dass dies nur für genehmigte Empfehlungen der guten Praxis gelten kann. Die KKA begrüsst sodann Abs. 2 von Art. 9. Dieser Absatz verdeutlicht, dass Empfehlungen nicht vollumfänglich rechtsverbindlich sein können.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	12			Art. 12 betrifft die ambulant tätige Ärzteschaft in doppelter Hinsicht: Wegen des kostenlosen Einsichtsrechts und wegen der Aufweichung des Berufsgeheimnisses. Jede Ärztin, jeder Arzt besitzt besondere schützenswerte Daten der Patientinnen und Patienten, dies namentlich auch in der Form der Krankengeschichte. Stirbt ein Patient oder eine Patientin, stellt sich die Frage des Umgangs mit diesen Daten insbesondere dann, wenn Dritte, namentlich Erben, Einblick in die Daten verlangen. Derzeit gilt, dass das Arztgeheimnis Ärztinnen und Ärzte dazu verpflichtet, im Grundsatz die Privatsphäre ihrer ehemaligen Patientinnen und Patienten, die verstorben sind, zu achten, es sei denn, eine Güterabwägung würde zu einem anderen Resultat führen. Diese Regelung schützt das Arztgeheimnis und vor allem auch die Rechte der Patientinnen und Patienten. Art. 12 will das bisher existierende Regel/Ausnahmeverhältnis ins Gegenteil verkehren, dies zumindest bei Ehepartnern, Partner einer eingetragenen Partnerschaft und bei Nachkommen: Sofern die verstorbene Person nicht ausdrücklich die Einsicht untersagt hat, ist der Arzt, ist die Ärztin als Verantwortliche verpflichtet, einen entsprechenden Einblick zu gewähren. Die KKA ist der Auffassung, dass das Regel-Ausnahmeverhältnis nicht umgekehrt werden sollte, denn

					eigentliche Missstände sind nicht bekannt. Der Arzt soll weiterhin die Interessen seines verstorbenen Patienten, seiner verstorbenen Patientin wahren können. Insbesondere der Umstand, dass bei bestimmten Kategorien ein schutzwürdiges Interesse vermutet wird, führt nach Auffassung der KKA zu erheblichen Schwierigkeiten. Bei gewissen Diagnosen, insbesondere im psychiatrischen Bereich, kann die vorgeschlagene Regelung zu sehr fragwürdigen Resultaten führen. Es geht hier auch um den postmortalen Persönlichkeitsschutz. Es steht einem Patienten offen, dem Arzt gegenüber zu erklären, dass im Falle seines Todes Verwandte und/oder die Nachkommen Einblick z. B. in die Krankengeschichte nehmen können. Das Arztgeheimnis und die Interessen der Patienten gebieten es indessen, dass das Geheimnis die Regel, die Bekanntgabe die Ausnahme sein soll.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13-16			Die Bedeutung dieser Bestimmungen für ambulant tätige Ärztinnen und Ärzte ist unklar. Es ist wohl davon auszugehen, dass Ärztinnen und Ärzte grundsätzlich Verantwortliche im Sinne des vorgeschlagenen neuen Datenschutzgesetzes sind. Die konkreten Auswirkungen sind indessen nicht absehbar. Die ausgedehnten Informationspflichten sind auf jeden Fall aus Sicht der KKA im Verhältnis zwischen ambulant tätigen Ärztinnen und Ärzten und ihren Patienten dem ärztlichen Behandlungsverhältnis nicht angemessen. Die KKA ist der Auffassung, dass sich die Ermächtigung zur Beschaffung von Personendaten und deren Weiterleitung als Teil der medizinischen Behandlung aus dem Behandlungsverhältnis ergibt. Es scheint zumindest, dass Informationspflichten, und zwar ausdrückliche, dann bestehen, wenn ein Grundversorger den Patienten an einen Spezialisten überweist, sodann im Verhältnis zwischen Belegarzt und Spital, möglicherweise bei der Behandlung eines Falles in einem Medical Board etc. Dies ist nicht erforderlich. Art. 13 ff. sind daher Beispiele von Regelungen, welche im Gesundheitsbereich in Empfehlungen der guten Praxis zumindest teilweise relativiert werden sollten. Dies setzt allerdings voraus, dass der Beauftragte in einem Genehmigungsentscheid von der Beachtung einzelner Bestimmungen des DSG dispensieren kann. Vergleiche hierzu auch die Stellungnahme zu Art. 8 DSG. Ähnliche Vorbehalte wie zu den Artikeln 13-15 ergeben sich bei Art. 16. Bedeutet die Bestimmung, dass sämtliche ambulant tätige Ärztinnen und Ärzte eine Datenschutz-Folgenabschätzung vornehmen müssen? Aufgrund des Wortlautes von Art. 16 muss man davon ausgehen, zumal Ärztinnen und Ärzte in den Besitz besonders schützenswerter Daten ihrer Patientinnen und Patienten gelangen. Die Risiken und möglichen Folgen dürfen indessen bei den meisten Ärztinnen und Ärzte gleich sein. Die geforderte

					Folgenabschätzung gemäss Art. 16 Abs. 2 würde daher bei den meisten Ärztinnen und Ärzte genau gleich aussehen und wäre damit nicht mehr als die rein formale Erfüllung einer lästigen Pflicht, nicht aber eine echte Information. Vollends keinen Sinn macht in diesem Zusammenhang die Benachrichtigungspflicht an den Datenschutzbeauftragten. Abschliessend ist festzuhalten, dass die Bestimmung, zumindest was deren potentielle Anwendung im Gesundheitsbereich anbetrifft, völlig unklar ist und überdies potentiell einen erheblichen Aufwand verursachen kann. Dies gilt insbesondere für die ambulant tätige Ärzteschaft. Auch bei Art. 16 handelt es sich um eine Bestimmung, deren Einhaltung und Umsetzung bei der ambulant tätigen Ärzteschaft wohl erheblich zu relativieren ist, dies auf dem Wege von Empfehlungen der guten Praxis.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19			Diese Bestimmung zählt ebenfalls zu den Normen, deren Reichweite für die ambulant tätige Ärzteschaft völlig unklar ist. Ein Hausarzt ist Verantwortlicher im Sinne des Gesetzes. In seiner Funktion muss er immer wieder Patientendaten an Dritte weitergeben (Versicherer, Vertrauensarzt, Spital, Spezialist, etc.). Ist ernsthaft die Meinung, dass er in jedem Fall die Empfängerinnen und Empfänger von Daten über die Patienten im Sinne von Art. 19 Bst. b) zu informieren hat? Aus Sicht der KKA macht dies keinen Sinn.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	23			Dieser Artikel umschreibt die Persönlichkeitsverletzungen in einer Art und Weise, welche tätige Ärztinnen und Ärzte als Verantwortliche unmittelbar betrifft. Die sichere und effiziente Behandlung von Patienten und Patienten ist nicht möglich, ohne dass Ärztin und Arzt ein Profiling im Sinne dieses Gesetzes machen, und ohne dass sie Dritten besonders schützenwerte Personendaten bekannt geben. Dass diese im Interesse des Patienten gebotenen Datenbearbeitungen gemäss Art. 23 Abs. 2 lit. c bzw. d. eine Persönlichkeitsverletzung darstellen sollen, ist ein zu korrigierender Konstruktionsfehler des Gesetzesentwurfs.
Fehler! Verweisquelle konnte nicht	DSG	24			Die Problematik liegt vor allem an den Anforderungen mit Bezug auf die Einwilligung der Patientinnen und Patienten. Die ärztliche Tätigkeit wird auf jeden Fall sehr stark behindert, wenn jeweils immer

gefunden werden.					ausdrückliche Einwilligungen einzuholen sind. Auch hier zeigt sich wieder der alte Konflikt: Einerseits sind Gesundheitsdaten besonders schützenswerte Daten, auf der anderen Seite verlangen die Umstände, insbesondere der Gesundheitszustand von Patientinnen und Patienten, häufig, dass diese Daten weitergegeben werden, dies im Interesse des Behandlungserfolgs oder auch bei der Rechnungsstellung. Zu kritisieren ist sodann die Umschreibung "möglicherweise" in Art. 24 Abs. 2. Damit wird das Vorliegen von Rechtfertigungsgründen relativiert und eine Rechtsunsicherheit geschaffen. Entweder liegt ein Rechtfertigungsgrund vor oder nicht. So wie Abs. 2 von Art. 24 jetzt formuliert ist, wissen Datenbearbeiter nicht, ob sie nun Daten zulässigerweise bearbeiten oder die Persönlichkeit Betroffener verletzen. Mit der Formulierung werden nur Rechtstreitigkeiten gefördert. Zu beachten sind in diesem Zusammenhang auch die verschärften Strafbestimmungen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	26-36			Die besonderen Bestimmungen für die Datenbearbeitung durch Bundesorgane im 6. Abschnitt des Gesetzesentwurfes sind für die ambulant tätige Ärzteschaft nicht unmittelbar relevant. Allerdings sind sie sonst im Gesundheitswesen von erheblicher Bedeutung, handelt es sich doch um Bestimmungen, an welche sich die Krankenversicherer in Vollzug des KVG bzw. im Vollzug der Grundversicherung zu halten haben. Ferner – dies darf nicht übersehen werden – bearbeiten Bundesorgane, eben zum Beispiel die Krankenversicherer, aber auch das BAG und weitere Bundesämter die wirtschaftlichen Daten der frei praktizierenden Ärztinnen und Ärzte als Leistungserbringer. Art. 29 Abs. 3 lit. b sieht vor, dass Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben dürfen, wenn an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Mit Bezug auf letzteres möchte die FMH klar festhalten, dass nach ihrer Auffassung nie ein öffentliches Interesse daran besteht, die finanziellen Daten einzelner in freier Praxis tätiger Ärztinnen und Ärzte zu veröffentlichen. Vorbehalte bestehen auch bezüglich von Art. 29 Abs. 4. Diese aus dem bisherigen Recht übernommene Regelung sieht vor, dass Bundesorgane auf Anfrage Name, Vorname, Adresse und Geburtsdatum von Personen bekanntgeben dürfen. Dies ist heute kritisch zu hinterfragen. Auch in einem solchen Falle muss ein legitimes Interesse an der Bekanntgabe bzw. an der Kenntnisnahme dieser Daten bestehen und eine Interessenabwägung stattfinden. Wenn sich jemand zum Beispiel aus Sicherheitsgründen nicht im

					Telefonbuch eintragen lässt, sollten Name, Vorname, Adresse und Geburtsdatum vom Bund nicht ohne stichhaltige Gründe bekanntgegeben werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	37-49			Die ambulant tätige Ärzteschaft wird durch die neuen Bestimmungen zum eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten nicht unmittelbar bzw. nicht besonders betroffen. Ungeklärt ist indessen aus Sicht der KKA das Verhältnis zwischen den Untersuchungsmassnahmen gemäss Art. 41 des Gesetzesentwurfs und die Geltung des Arzt- bzw. Patientengeheimnisses. Die KKA geht davon aus, dass auch im Falle von Untersuchungen, welche sich gegen eine einzelne Ärztin bzw. gegen einen einzelnen Arzt richten, dieser sich auf das Arztgeheimnis berufen kann. Wäre dem anders, so müsste dies ausdrücklich im Gesetz geregelt sein. Die KKA wäre gegen eine solche Regelung.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	50-55			Der Entwurf sieht eine massive Ausweitung der strafrechtlichen Sanktionen im Vergleich zur geltenden Regelung in Art. 34 und 35 DSG vor. Die RL (EU) 2016/680 vom 27. April 2016, also die neue Datenschutzlinie der EU verlangt solches nicht. Sie hält in Art. 57 unter dem Titel "Sanktionen" allein fest: Die Mitgliedstaaten legen fest, welche Sanktion bei einem Verstoss gegen die nach dieser Richtlinie erfassten Vorschriften zu verlängern sind, und treffen die zu deren Anwendung erforderlichen Massnahmen. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein.“ Das ist alles. Der Entwurf regelt demgegenüber in sechs, zum Teil umfangreichen Artikel die strafrechtlichen Sanktionen. Die KKA ist der Auffassung, dass ein derart umfangreicher Strafkatalog nicht erforderlich ist. Überdies sind die Strafnormen zum Teil wenig präzise abgefasst bzw. können Anlass geben für unnötige, auch belastende Strafverfahren. Klar handelt es sich zu einem erheblichen Teil um Antragsdelikte. Dies ändert aber nichts daran, dass ein Strafverfahren eingeleitet werden kann, dies mit den möglichen Folgen für die Betroffenen. Strafrechtlich verfolgt werden können gemäss dem Entwurf private Personen, was juristische und natürliche Personen einschliesst. Allerdings ist die Möglichkeit der Bestrafung juristischer Personen gestützt auf Art. 53 des Entwurfes eingeschränkt und nur möglich, wenn der Bussenbetrag CHF 100'000.- nicht überschreitet und die Ermittlung der verantwortlichen natürlichen Person unverhältnismässig wäre. Es bleibt abzuwarten, was insbesondere letztere Umschreibung zu bedeuten haben wird. Auf jeden Fall ergibt sich aus den vorgeschlagenen Gesetzesnormen, dass die strafrechtliche Verantwortung natürlicher Personen die Regel und die Möglichkeit der Bestrafung juristischer Personen die Ausnahme darstellen soll. Dies bedeutet insbesondere, dass auch einzelne Ärztinnen und einzelne Ärzte sich strafbar machen

					können. Mithin sind die Strafbestimmungen für die ambulant tätige Ärzteschaft von erheblicher Bedeutung, ist doch auf deren Tätigkeit – wie bereits gesehen – das DSG grundsätzlich anwendbar.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	50			Die fehlende Präzision der vorgeschlagenen Strafnormen zeigt sich bereits bei Art. 50 Abs. 1. Die Erteilung einer unvollständigen Auskunft kann mit Busse bis zu CHF 500'000.- bestraft werden. Wann ist eine Auskunft unvollständig? Auch eine eventual vorsätzlich begangene unvollständige Auskunft führt zur Bestrafung. Die Abgrenzungsprobleme sind programmiert. Dieselbe Problematik ergibt sich auch bei der Verletzung von Informationspflichten. Ein gutes Beispiel einer wirklich missglückten Strafnorm ist die in Art. 50 Abs. 1 lit. e vorgesehene Möglichkeit einer Bestrafung mit Busse bis zu CHF 500'000.-, dies nicht nur auf Antrag, bei der Unterlassung, dem Beauftragten Verletzungen des Datenschutzes nach Art. 17 Abs. 1 zu melden. Art. 17 Abs. 1 sieht eine Meldepflicht vor bei einer unbefugten Datenbearbeitung oder beim Verlust von Daten, macht dann aber einen Vorbehalt, dies für den Fall, dass ein Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person "voraussichtlich" ausbleibt. Es muss also nicht immer in jedem Fall gemeldet werden, vielmehr kann eine Abwägung vorgenommen werden. Es macht keinen Sinn, derartige Normen mit einer strafrechtlichen Sanktionsmöglichkeit zu versehen. In vielen Fällen genügt es, anstelle einer strafrechtlichen Drohung dem Beauftragten die Möglichkeit zu geben in der Sache zu verfügen und die Nichteinhaltung der Verfügung mit StGB Art. 292 abzusichern. Auch die in Art. 51 des Entwurfes vorgesehenen Strafmöglichkeiten bei Verletzungen von Sorgfaltspflichten können ohne weiteres durch Verfügungen des Beauftragten ersetzt werden, welche mit StGB Art. 292 abgesichert werden können, sollte dies erforderlich sein. Nach Ansicht der KKA muss der Katalog der Strafnormen nochmals umfassend überdacht werden. Von diesem Katalog wären vor allem Personen betroffen, welche in Unternehmungen für den Datenschutz verantwortlich sind. Die Strafnormen sind derart unpräzise und weit gefasst, dass derartige Personen auch angesichts der Komplexität von Datenschutzfragen insbesondere im Gesundheitsbereich ein hohes Risiko laufen, in Strafverfahren verwickelt zu werden. Die KKA erachtet dies als nicht sinnvoll.
Fehler! Verweisquelle konnte nicht	DSG				

gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler!	

Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Geschäftsstelle
Kappelergasse 14
8001 Zürich

T +41 44 211 40 11
F +41 44 211 80 18
info@ks-cs.ch

ks/cs
Kommunikation Schweiz
Communication Suisse
Comunicazione Svizzera
Communication Switzerland

Per E-Mail an jonas.amstutz@bj.admin
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 4. April 2017

Stellungahme von KS/CS zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

KS/CS Kommunikation Schweiz ist 1925 als erster Verband der Werbebranche gegründet worden und steht im Dienste ihrer Mitglieder, den Werbeagenturen, Werbeauftraggebern und Medienanbietern. Weiter integriert in den Dachverband der kommerziellen Kommunikation sind neben Unternehmen verschiedene Branchenverbände sowie wichtige Wirtschaftsverbände. Die Schweizer Werbebranche erwirtschaftet gemäss einer Studie aus dem Jahr 2013 pro Jahr rund 7.2 Milliarden Franken Netto-Umsatz – das entspricht etwa 1.34 % des Bruttoinlandproduktes), alimentiert annähernd 21‘700 Vollzeitstellen und generiert rund 168 Millionen Franken Steuereinnahmen.

A. Einleitende Gedanken zum Datenschutz und zum vorliegenden Gesetzesentwurf

Für jedes Unternehmen in der Schweiz ist es von existenzieller Bedeutung, mit seinen aktuellen oder potenziellen Kunden, seinen Zulieferern und sonstigen Partnern möglichst wirkungsvoll kommunizieren zu können. Dabei werden naturgemäss Personendaten ausgetauscht. Das Kommunizieren ist für Unternehmen sozusagen der Sauerstoff ihrer wirtschaftlichen Tätigkeit.

Das Datenschutzgesetz hat demzufolge für sämtliche Unternehmen sowie die davon abhängigen Arbeitnehmerinnen und Arbeitnehmer eine existenzielle Bedeutung, insbesondere im Bereich der digitalen Kommunikation. Der Bundesrat hat dies erkannt und im Zusammenhang mit seinem am 11. Januar 2017 verabschiedeten Bericht «Rahmenbedingungen der digitalen Wirtschaft» verlauten lassen:

> ***«Der digitale Wandel bietet grosse Chancen für die Schweizer Volkswirtschaft. Der Bundesrat will diese nutzen, um Arbeitsplätze und Wohlstand zu sichern.»***

Der vorliegende Gesetzesentwurf widerspricht diesem Vorhaben des Bundesrates, den Wirtschaftsstandort Schweiz und den allgemeinen Wohlstand zu fördern, diametral! Er bewirkt vielmehr einen gravierenden Standortnachteil, der neben Grossunternehmen insbesondere die heimischen KMUs überfordert und existenziell gefährdet.

B. Grundposition zum vorliegenden Gesetzesentwurf

KS/CS anerkennt und erachtet es als notwendig, dass das aktuelle DSG dahingehend überarbeitet wird, dass die Vorgaben der Europarats-Konvention (E-SEV 108) und ein anerkennungsfähiges Schutzniveau im Lichte der EU-DSGVO erfüllt werden, um den internationalen Datenaustausch zu ermöglichen resp. zu vereinfachen. Diese internationalen Bestimmungen legen ein allgemein anerkanntes Schutzniveau im Bereich Datenschutz fest.

Vor diesem Hintergrund lautet die Position von KS/CS wie folgt:

Das Datenschutzgesetz ist insoweit zu revidieren, als es die internationalen Vorgaben zwingend erfordern. Jeder darüber hinausgehender «Swiss Finish» (im vorliegenden Entwurf zum Beispiel besonders gravierend im Bereich Profiling und Sanktionensystem) ist strikte abzulehnen.

C. Einzelne zentrale Punkte

I. Art. 3 Bst. a DSG, Begriff der Personendaten

Die Beibehaltung der Definition von Personendaten ist zu begrüssen.

Unter Einbezug des erläuternden Berichts ist die vorgeschlagene Regelung jedoch unklar und potenziell widersprüchlich. Auf der einen Seite soll der Begriff «Personendaten» gegenüber dem geltenden Recht zwar inhaltlich nicht geändert werden; dabei ist insbesondere die implizite Anerkennung der relativen Methode, wie sie auch in der EU künftig weiterhin gelten soll, zentral und richtig. Auf der anderen Seite wird im Bericht eine natürliche Person als bestimmbar erklärt, wenn sie «über Hinweise auf eine Identifikationsnummer oder eine Online-Identität» identifiziert werden kann.

Diese Formulierung ist gerade in diesem Punkt, der für sämtliche Online-Aktivitäten fundamental ist, missverständlich und je nach Interpretation widersprüchlich. Denn nach der wohl herrschenden Auffassung genügt es unter dem geltendem DSG für eine eindeutige Identifizierung nicht, wenn Angaben bloss einer bestimmten «eindeutigen Kennung» oder «Identifikationsnummer», z.B. einer IP-Adresse oder Cookie-Kennung, zugeordnet werden können, hinter der letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann (sog. Singularisierung). Bei der Qualifikation von IP-Adressen usw. muss daher auch künftig eine Einzelfallbeurteilung entscheidend sein, die sowohl den Aufwand für die Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektive Seite) berücksichtigt wie auch das Interesse an der Identifizierung (subjektive Seite).

Insbesondere beim Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites, bei dem regelmässig auch die IP-Adresse mitbearbeitet wird, besteht kein Interesse an der namentlichen Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten. Letzten Endes würden zahlreiche unentgeltliche, heute werbefinanzierte Angebote künftig nicht mehr allgemein zur Verfügung stehen. Vor diesem Hintergrund ist es entscheidend, in der Botschaft klarzustellen, dass das Konzept der Singularisierung abgelehnt wird. Der Umstand, dass nach Auffassung einzelner Autoren unter der EU-DSGVO eine Singularisierung für das

Vorliegen von Personendaten ausreichen soll, ändert daran nichts. Denn zum einen wird diese Auffassung von anderen Autoren mit überzeugenden Argumenten abgelehnt. Zum anderen ergibt sich eine derart strenge Auslegung auch nicht aus dem E-SEV 108. Deshalb besteht keine Notwendigkeit, sie im Schweizer Recht einzuführen (Swiss Finish).

II. Art. 3 Bst. f DSG, Begriff des Profiling

Die vorgeschlagene Definition und die damit einhergehende Regelung (siehe dazu Anmerkungen zu Art. 23 unten) des «Profiling» werden abgelehnt. Die Definition geht ohne Not weit über diejenige der EU-DSGVO (Art. 4 Ziff. 4) hinaus (Swiss Finish).

Zudem enthält der E-SEV 108 keinerlei Vorgaben für das Profiling. Vielmehr verlangt dieser nur eine Regelung von automatisierten Entscheidungen (vgl. Art. 8 Abs.1 lit. a). Ausgehend davon sollte auf spezifische Vorgaben für das Profiling verzichtet werden. Wird gleichwohl an einer Regelung festgehalten, sollte diese aber jedenfalls auf automatisierte Bearbeitungen beschränkt bleiben. Keinesfalls darf die Regelung jedoch derart weit gefasst werden, dass die Vorgaben (systemwidrig) sogar für das Profiling mit nicht personenbezogenen Daten gelten. Für die im erläuternden Bericht angesprochenen Bearbeitungen beispielsweise im Rahmen von Big-Data-Analysen genügen die übrigen Regelungen vollends. Denn bei einem Profiling, das am Ende zu Personendaten führt, gelten diese ohnehin bereits. Darüber hinaus würde die Unsicherheit, welche konkreten Bearbeitungen in der Praxis als Profiling zu betrachten sind, durch den entsprechenden Zusatz weiter verstärkt.

III. Art. 6 Abs. 1 Bst. b DSG, Begriff der Einwilligung

Die vorgeschlagene Änderung hinsichtlich des überaus zentralen Begriffs der «Einwilligung» ist unklar. Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit auch eine inhaltliche Annäherung bezweckt wird. **Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung. Eine klare Regelung und damit Rechtssicherheit ist deshalb entscheiden.**

Die gegenüber der E-SEV 108 unnötig strengen Vorgaben der EU-DSGVO in Bezug auf die «Freiwilligkeit der Einwilligung» (Art. 7 Abs. 4) zu übernehmen, würde die Rechtslage gegenüber dem geltenden Recht massiv verschärfen sowie die Vertragsfreiheit erheblich einschränken. Das ist unnötig und daher abzulehnen. Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss («free consent»), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben. In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden.

Darüber hinaus sind die Ausführungen im erläuternden Bericht zur «ausdrücklichen Einwilligungen» unklar bzw. unvollständig. Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden. Das ist gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch. Es ist daher in der Botschaft auch klarzustellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn die Datenbearbeitung, in die eingewilligt wird, also z.B. das Profiling, in einer Datenschutzerklärung beim Namen genannt wird. Insofern würde es nicht genügen, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste.

Schliesslich ist in der Botschaft auch festzulegen, dass – entsprechend dem geltenden Recht – eine **Einwilligung in Datenbearbeitungen auch durch Zustimmung zu einem Dokument, das weitere Informationen erhält (z.B. AGB oder Datenschutzerklärungen), erteilt werden kann und in diesem Fall keine separate Information bzw. Einwilligung erforderlich ist.**

IV. Art. 7 DSG, Auftragsdatenbearbeitung

Es ist zu begrüssen, dass die geltende Rechtslage hinsichtlich der Auftragsdatenbearbeitung grundsätzlich beibehalten wird. Abzulehnen ist jedoch die unbeschränkte Delegation an den Bundesrat zur Festlegung weiterer Pflichten. Zudem ist Abs. 3 zu streichen. Eine zwingende Zustimmung zum Beizug von Sub-Auftragsdatenbearbeiter ist weder durch die internationalen Verpflichtungen gefordert, noch entspricht sie der bisher geltenden Rechtslage (Swiss Finish). Sie wäre in der Praxis auch nicht praktikabel. Sollte daran festgehalten werden, müsste die Bestimmung zumindest dahingehend angepasst werden, dass nicht «Schriftlichkeit» erforderlich ist, sondern eine Form, die den «Nachweis durch Text» ermöglicht. Andernfalls wäre die Ermächtigung zur Einsetzung von Unterauftragnehmern namentlich in Verträgen, die online abgeschlossen werden, nicht mehr möglich.

V. Art. 12 DSG, Daten einer verstorbenen Person

Die Einführung einer Regelung zu Daten verstorbener Personen ist im Hinblick auf die Angemessenheit des Schweizer Datenschutzrechts nicht zwingend erforderlich und würde für die Unternehmen zu einem erheblichen administrativen Mehraufwand (Swiss Finish) führen. **Auf die Regelung ist daher zu verzichten.**

VI. Art. 13 und Art. 15 DSG Informationspflicht

Eine generelle Informationspflicht einzuführen, ist mit Blick auf den E-SEV 108 zwingend und insofern richtig. **Allerdings gehen diverse Punkte der vorgeschlagenen Regelung zu weit und sind daher abzulehnen** (vgl. dazu die eingehende Stellungnahme des Schweizer Dialogmarketing Verbandes SDV).

VII. Art. 16 Datenschutz-Folgenabschätzung

Die Anknüpfung an das Vorliegen «erhöhter Risiken» würde zu einem viel zu weit gefassten Anwendungsbereich führen und ginge unverständlicherweise sogar über die Vorgaben in der EU-DSGVO (Art. 35) hinaus (Swiss Finish).

VIII. Art. 23 Abs. 2 Bst. d, Profiling nur mit Einwilligung

Dass eine ausdrückliche Einwilligung für das Profiling erforderlich sein soll, würde eine der problematischsten Schweizer Verschärfungen darstellen und ist zwingend zu streichen (Swiss Finish). Für die Werbewirtschaft hätte diese Anforderung erhebliche Konsequenzen, die unnötig, unangemessen und unzweckmässig wären. Das E-SEV 108 verlangt keine entsprechende Vorgabe. Ferner ist auch nach der EU-DSGVO nicht für jegliche Form des Profiling eine Einwilligung erforderlich. Das Profiling per se als Persönlichkeitsverletzung einzustufen, ist auch sachlich nicht notwendig. Solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll.

Wird diese Vorschrift Gesetz, verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung/personalisiertem Marketing und stellt eine Bedrohung für den Wirtschaftsstandort Schweiz dar. Profiling und damit personalisierte Werbung wäre dann faktisch nur noch den grossen – insbesondere internationalen – Log-in-Giganten wie Facebook, Google, Apple und Co. vorbehalten. Diese Unternehmen können sich meist problemlos auf eine ausdrückliche Einwilligung im Rahmen der Account-Registrierungen stützen. Die Folgen wären auch aus kartellrechtlichen Überlegungen höchst problematisch.

IX. Art. 50 ff. Sanktionensystem

Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt. Es wäre in höchstem Mass innovationshemmend und würde eine Kultur des Denunziantentums in den Unternehmen etablieren. Die Folge wäre ein ganz erheblicher Standortnachteil für die Schweiz. Kein innovatives digitales Start-Up beispielsweise würde bereit sein, seine Gründer und Mitarbeitenden solch drastischen strafrechtlichen Risiken auszusetzen. Gute Mitarbeitende würden nicht mehr bereit sein, Verantwortung in den Unternehmen mitzutragen.

Für die Berücksichtigung der Anliegen der Werbebranche zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung. Im Übrigen verweisen wir auf die weitergehend begründete Eingabe des Schweizer Dialogmarketing Verbandes SDV.

Freundliche Grüsse

Kommunikation Schweiz
Präsident

Ständerat Filippo Lombardi

Präsidenten und Vizepräsidentin Sektionen

Christian Merk	François Besençon	Maria Luisa Bernini
Sektion Deutschschweiz	Section Suisse Romande	Sezione Svizzera Italiana

LICENSING EXECUTIVES SOCIETY
SCHWEIZ SUISSE SVIZZERA SWITZERLAND

Département fédéral de justice et police
3003 Bern

Par courriel uniquement: *jonas.amstutz@bj.admin.ch*

Président LES-CH:
Raymond Reuteler
c/o reuteler & cie SA
ch. Vuarpillière 29
CH-1260 Nyon

T: +41 22 363 79 40
raymond.reuteler@reuteler.net

Le 15 Mars 2017

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Madame, Monsieur,

LES-CH est une association de droit suisse qui aborde tous les aspects de la protection et de la commercialisation de la Propriété Intellectuelle (PI) avec une approche orientée vers le monde de l'entreprise.

LES-CH, qui compte parmi ses membres des dirigeants d'entreprises, des scientifiques, des ingénieurs, des académiques, des avocats et des conseils en propriété intellectuelle, représente un regroupement riche et unique de professionnels du monde des affaires, de secteurs techniques variés et du domaine légal. Avec près de 300 membres, LES-CH est l'une des plus grandes associations en matière de propriété intellectuelle en Suisse.

LES-CH soutient les politiques publiques qui favorisent les droits de propriété forts et un système juridique fiable.

Dans le cadre de ses activités, le LES-CH a pris connaissance de l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données (ci-après "ALPD") qui prévoit dorénavant de soumettre les registres publics de propriété intellectuelle à la loi sur la protection des données.

Dans le délai imparti au 4 avril 2017, l'association LES-CH conteste le bien-fondé de ce changement de paradigme visant à soumettre à l'ALPD les registres publics de propriété intellectuelle découlant notamment de la loi fédérale sur les marques et des indications de provenance géographiques, de la loi fédérale sur les brevets ("**LBI**") et de la loi fédérale sur les designs, tous gérés par l'Institut fédéral de la propriété intellectuelle.

A ce jour, une personne (physique ou morale) peut obtenir un monopole sur une marque, un brevet ou un design. La contrepartie automatique et obligatoire de ce monopole est la publicité

du registre et la consultation par tout tiers des pièces contenues dans ce même registre. Il s'agit de principes cardinaux essentiels à la viabilité du système puisqu'ils sont les seuls à même de permettre la transparence - et donc le contrôle - du système. Les seules limitations actuelles portées à ces deux principes sont (i) la garantie de pouvoir classer à part les documents qui contiennent des secrets de fabrication ou d'affaires (art. 36 al. 3 de l'Ordonnance sur la protection des marques ("**OPM**"), art. 65 LBI, art. 22 de l'Ordonnance sur les designs ("**Odes**")) et la destruction des documents suite à une radiation/révocation du droit de propriété intellectuel (art. 39 OPM, art 92 OBI, art. 24 ODes). Les utilisateurs du système sont ainsi parfaitement informés du fait que les données communiquées dans le cadre d'une procédure devant l'Institut fédéral de la propriété intellectuelle sont entièrement accessibles au public.

Le LES-CH est d'avis que l'application de l'ALPD aux registres publics de propriété intellectuelle est inappropriée car elle ne permet pas de tenir compte de (i) l'intérêt public général à pouvoir accéder à toutes les données échangées en vue de l'octroi d'un monopole et (ii) des deux principes cardinaux précités. Ce constat ne signifie pas que la protection des données ne doit pas trouver du tout d'application dans le domaine de la propriété intellectuelle, mais elle doit s'effectuer par des dispositions spéciales, contenues directement dans les lois spécifiques de propriété intellectuelle. Seule une telle approche permet de tenir compte des particularités des divers droits de propriété intellectuelle et de régler, en fonction du registre (marque, indications géographies, brevet, design, etc.), les questions relatives à la protection des données.

Au surplus, la tendance actuelle est très clairement de permettre un accès immédiat online à l'ensemble du dossier. Cette pratique est largement répandue au niveau européen et tant l'Office de l'Union européenne pour la propriété intellectuelle que l'Office Européen des Brevets offrent un accès électronique online à l'ensemble des pièces de la procédure, y compris les échanges entre les parties et entre les parties et l'office. Les utilisateurs suisses du système militent pour qu'une telle offre soit aussi disponible pour les registres publics suisses de propriété intellectuelle, ce qui permettra d'accroître encore la transparence et l'efficacité du système. Il va sans dire que l'application de l'ALPD à ces registres va entraver inutilement un tel développement.

Pour les motifs précités, le LES-CH est d'avis que la suppression de l'exception prévue actuellement à l'article 2 al. 2 let. d LPD n'a aucune raison d'être et demande que cette exception perdure, à tout le moins pour les registres publics de droits de propriété intellectuelle.

En vous remerciant de l'attention que vous porterez à la présente, je vous prie de croire, Madame, Monsieur, à mes salutations distinguées.

Raymond Reuteler

LAUX LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

RECHTSANWÄLTE
Z Dr. Christian Laux · LLM
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

In den zuständigen Anwaltsregistern eingetragen

P.O. Box 360, CH 8024 Zürich

per Email zu Handen: jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundeshaus West
3003 Bern

4. April 2017

Stellungnahme zum Vorentwurf zur Totalrevision des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

LAUX LAWYERS AG ist eine Anwaltskanzlei mit Fokus IT-Recht. Unsere Aufgabe sehen wir darin, durch spezialisierte Fachkompetenz an der Schnittstelle zwischen Recht und IT den IT-Sektor zu unterstützen. Mit dieser Aufgabenstellung beraten wir unter anderem sowohl Kunden und Nutzer von Outsourcings als auch Anbieter von solchen Leistungen (kundenindividuelle Auslagerungen, Cloud Computing und Managed Services).

Mit dieser Eingabe nehmen wir Stellung zur Vernehmlassungsvorlage betreffend Totalrevision des Datenschutzgesetzes (VE-DSG, gemäss Mitteilung des Bundesrats vom 21. Dezember 2016).

Wir erlauben uns, in Bezug auf die in Anhang 1 kommentierten Bestimmungen des VE-DSG zu schildern, inwiefern diese die Digitalisierungsbestrebungen in der Schweiz beeinträchtigen würden. Dabei beschränken wir uns auf Kommentare zum eingangs erwähnten „Cloud Computing". Wir hoffen, mit diesem fokussierten Beitrag die Diskussion zum VE-DSG bereichern zu können.

A. Zum Cloud Computing und seiner Bedeutung für den Datenschutz

1 Cloud Computing ist ein Sammelbegriff für technische IT-Infrastrukturen, die zusammen mit ergänzenden Dienstleistungen für die Digitalisierung der Schweiz von grösster Bedeutung sind. Das massgebliche Merkmal solcher Dienstleistungen besteht darin, dass dank standardisierter Technologie sowie standardisierten, ergänzend bereitgestellten Dienstleistungen vermehrt softwareunterstützte Prozesse zur Verfügung stehen oder abgebildet werden können, für die ein Kunde zuvor ungleich grössere finanzielle Mittel hätte aufwerfen müssen.

2 Dies bedingt, dass der Cloud-Anbieter sich für eine Vielzahl von Kunden so organisiert, dass er gleichartige IT-Infrastrukturen und gleichartige Prozesse allen Kunden unterschiedslos zur Verfügung stellen kann. Der Anbieter sorgt mittels technischer, organisatorischer und vertraglicher Massnahmen dafür, dass seine eigenen Mitarbeitenden nicht auf Daten von Kunden Zugriff nehmen und dass einzelne Kunden nicht auf Daten von anderen Kunden Zugriff nehmen können.

3 Je nach Situation und der vom Anbieter gewährten Transparenz kann der Kunde die vom Cloud-Anbieter getroffenen technischen und organisatorischen Massnahmen direkt nachvollziehen. Zusätzlich sichert der Cloud-Kunde seine Schutzziele – Schutz vor unbefugtem Zugriff, Schutz vor unbefugter Verwertung und Integritäts- sowie Verfügbarkeitsschutz – vertraglich ab. Dabei unterscheiden sich Cloud-Angebote für die Geschäftsnutzung erheblich von Angeboten, die sich an den Endkunden (Konsumenten) richten.

4 Erscheinungsformen:

> ***IaaS**: Ein Kunde verwaltet nicht mehr wie bis anhin eigene Hardware und Plattformsoftwares, um anschliessend Applikationen zur eigenen Nutzung zu installieren. sondern wird vom Cloud-Anbieter im Resultat gleichgestellt, indem dem Kunden sog. Virtuelle Server („Virtual Machines") zur Verfügung gestellt werden. Der Cloud-Anbieter setzt aber zu diesem Zweck IT-Infrastrukturen ein. zu deren Schutz er die technisch und organisatorisch relevanten Massnahmen ergreift. Man spricht hier von Infrastructure as a Service (oder IaaS). weil dem Kunden die Aufgabe abgenommen wird, selber den Standort des Servers zu bestimmen. die Hardware auszuwählen und lauffähig zu erhalten. Der Kunde bleibt aber in der Verantwortung. die Virtuelle Maschine so mit Betriebssystemen auszustatten. dass sie für ihn nützlich ist. Einblick des Cloud-Anbieters in die Virtuelle Maschine (und damit Einsicht in Daten) ist technisch nicht erforderlich, dass das IaaS-Angebot dem Kunden nützlich ist.*
>
> ***PaaS**: Wenn der Cloud-Dienstleister dem Kunden darüber hinaus weitere Verwaltungstätigkeiten abnimmt (gleich wie zuvor der IT-Dienstleister, der dem Kunden über Remote-Zugriff von aussen geholfen hat, Betriebssysteme. Datenbanken und dergleichen in Stand zu halten), spricht man von Platform as a Service (PaaS). Der Kunde kann sich darauf beschränken, die für ihn relevanten Applikationen aufzusetzen, so dass sie ihm nützlich sind. Cloud-Anbieter, die nach modernen Verfahren organisiert sind. erbringen die Verwaltungstätigkeiten zum Betrieb der Plattformsoftwares mit Hilfe von automatisierten Prozessen und müssen entsprechend keinen kundenspezifischen Einblick in Daten von Kunden erhalten, um den Service anbieten zu können.*
>
> ***SaaS**: Ähnlich wie im PaaS-Konzept stellt der SaaS-Anbieter (SaaS für „Software as a Service") direkt nutzbare Software zur Verfügung. Der Cloud-Anbieter hat im SaaS-Modell die vom Kunden genutzte Applikation allerdings bereits vorinstalliert und nutzbar gemacht. Der Kunde kann sich darauf beschränken, die Applikation zu bedienen; allenfalls kann er sie anhand von vorhandenen Parametern auf seine Bedürfnisse einstellen.*

5 Beispiele für Cloud-Angebote, die sich an Geschäftskunden richten:

> ***IaaS**: Ein Unternehmen bezieht reine IT-Infrastrukturleistungen vom Anbieter, betreibt die darauf zu installierende Betriebssystemsoftware und Applikationen aber selber / durch eigenes Personal.*
>
> ***SaaS**: Ein Unternehmen bezieht eine Applikation zur Arbeitszeitenerfassung und zur Verwaltung weiterer Personalfragen über einen Dienstleister. Die inhaltliche Bearbeitung nimmt allein das Unternehmen vor.*

6 Beispiel für Cloud-Angebote, die sich an Konsumenten richten:

> ***SaaS**: Ein Konsument benutzt einen Cloud-Dienst, um seine Fotos an zentraler Stelle abzulegen.*

B. Relevante Bestimmungen im VE-DSG aus Kundensicht

7 Aus Kundensicht stellen sich gemeinhin vier wesentliche Kernfragen, die unter anderem unter http://www.cloudprivacycheck.eu schematisch und übersichtlich dargestellt sind:

- Daten unter Dritteinfluss: Sind Datenschutzaspekte zu beachten, weil der Cloud-Kunde Daten bearbeitet, in Bezug auf welche er gegenüber Dritten Rechenschaft ablegen muss?
- Beizug eines Dritten / Technische und organisatorische Massnahmen: Welche IT-Infrastrukturen betreibt der Cloud-Anbieter und welche technischen und organisatorischen Massnahmen ergreift er?
- Datenhaltung im Ausland oder Datenzugriff aus dem Ausland: Inwiefern entsteht durch die Nutzung des Cloud-Anbieters bzw. der von ihm bereitgestellten Dienste ein Auslandbezug?

- Subunternehmer: Inwiefern stellt der Cloud-Anbieter auf Subunternehmer ab?

8 Der Vorentwurf beschlägt diesen Fragekatalog wie folgt:

- Daten unter Dritteinfluss: Der Begriff der Personendaten wird enger gefasst (keine Regelung von Unternehmensdaten; insofern wird der Anwendungsbereich von Daten unter Dritteinfluss reduziert, was zu begrüssen ist). Die Regelung verbessert den Handlungsspielraum für Cloud-Kunden.

- Beizug eines Dritten / Technische und organisatorische Massnahmen: Als besonders störend ist die Regelung von Art. 13 Abs. 4 VE-DSG hervorzuheben. Die dort postulierte Mitteilungspflicht ist systemwidrig, hat keinen Mehrwert und führt wohl in aller Regel gar zu Mitteilungen, welche die betroffene Person über den tatsächlichen Schutz ihrer Personendaten in die Irre führen können.

- Datenhaltung im Ausland oder Datenzugriff aus dem Ausland: Der Beizug von Dienstleistern aus dem Ausland wird erschwert (erschwerte Planung wegen z.T. komplizierterer Regelungen).

- Subunternehmer: Würde Art. 7 Abs. 3 VE-DSG nicht „europakompatibel" gelesen werden können (nämlich: nachträgliche Meldung genügt, solange der Cloud-Anbieter generell im Vertrag ermächtigt ist, Subunternehmer beizuziehen), würde die Stellung des Cloud-Kunden auf den ersten Blick zwar verbessert; insgesamt würde die wenig hilfreiche Regelung allerdings das Leistungsangebot für Cloud-Kunden reduzieren (weil weniger Anbieter bereit wären, zu diesen Bedingungen Cloud-Angebote an Kunden in der Schweiz zu erbringen). Ein Cloud-Kunde, dem der Cloud-Anbieter Transparenz über beigezogene Dienstleister verspricht, ist auf die strengere („nicht europakompatible") Lesart aber nicht angewiesen, um Kontrolle über den Dienstleister und das Leistungsangebot auszuüben.

9 Bestimmungen, die den Cloud-Kunden einschränken, sind zu vermeiden, da sie die Digitalisierungsbestrebungen der Schweiz bremsen und die Wettbewerbsfähigkeit der Schweiz beeinträchtigen. Wir verweisen für detaillierte Kommentare hierzu auf Anhang 1 zu diesem Schreiben.

C. Relevante Bestimmungen im VE-DSG aus Anbietersicht

10 Aus Anbietersicht enthält der Vorentwurf gewisse Bestimmungen, welche die Rollenteilung zwischen Auftragsdatenbearbeiter und Verantwortlichem verwischen, ohne dass dazu ein Anlass bestünde. Zu nennen sind:

- Art. 16 VE-DSG: Datenschutzfolgeabschätzung sollte ein Cloud-Anbieter nur vornehmen müssen, wenn er Verantwortlicher ist. Ist er allein als Auftragsdatenbearbeiter tätig, trifft die Pflicht zur Datenschutzfolgeabschätzung allein den Cloud-Kunden (als Verantwortlichen).

- Art. 17 VE-DSG: Die (strafbewehrten) Pflichten, eine Data Breach Notification abzusetzen, sollten den Cloud-Anbieter (als Auftragsdatenbearbeiter) nur in der ihn betreffenden Risikosphäre treffen. Diese sollte präzisiert werden.

- Art. 18 VE-DSG: Privacy by Design sollte dem Cloud-Anbieter nicht als eigene Pflicht auferlegt werden (solange er nur als Auftragsdatenbearbeiter tätig ist); aber selbstverständlich wird der Cloud-Anbieter den Verantwortlichen bei der Umsetzung von solchen Massnahmen unterstützen müssen.

- Art. 19 lit. b VE-DSG: Die in Art. 19 lit. b VE-DSG genannten Informationspflichten könnte der Cloud-Anbieter nicht wahrnehmen, wenn er das oberste Ziel (keinen Zugriff auf Daten des Cloud-Kunden) umsetzt. Die Regelung steht insofern in grellem Kontrast zu den technischen und organisatorischen Massnahmen, die für seriöse Cloud-Anbieter als State of the Art bezeichnet werden können.

- Art. 20 Abs. 5 VE-DSG: Die Regelung würde die Attraktivität des Standorts Schweiz für Cloud-Anbieter erheblich beeinträchtigen.

11 Detaillierte Anmerkungen zu diesen Bestimmungen finden sich wiederum in Anhang 1 zu diesem Schreiben.

12 Gesamthaft lässt sich festhalten, dass der Vorentwurf den Auftragsdatenbearbeiter nicht nur als ausführende Stelle behandelt, die zur Einhaltung von Weisungen des Verantwortlichen verpflichtet ist, sondern ihn in Verkennung der Gesetzessystematik darüber hinaus als eigenständigen Risikoträger behandelt. Wir halten dies nicht für empfehlenswert. Die Rechtsbeziehung zwischen Cloud-Anbieter und Cloud-Kunde sollte abschliessend durch Art. 7 und Art. 11 VE-DSG geregelt sein.

* * *

Abschliessend bitten wir Sie höflich um positive Auseinandersetzung mit unseren Vorschlägen. Gerne stehen wir für allfällige Präzisierungen zur Verfügung. Für Ihre Bemühungen danken wir Ihnen bestens.

Freundliche Grüsse

Christian Laux Alexander Hofmann

Anhang 1: Ausformulierte Kommentierungen und Anpassungsvorschläge

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : LAUX LAWYERS AG, Zürich

Abkürzung der Firma / Organisation : LLAG
Adresse : Seegartenstrasse 2, Postfach 360, 8024 Zürich
Kontaktperson : RA Dr. Christian Laux
Telefon : 044 880 24 24
E-Mail : christian.laux@lauxlawyers.ch
Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2. Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
LAUX LAWYERS AG [LLAG-1]	Wir verweisen hier auf unser Begleitschreiben und die diesem angehängten Separatdokumente. Wir bitten Sie höflich um inhaltliche Auseinandersetzung mit diesen und würden uns freuen, diese im Gespräch bei Bedarf zu verdeutlichen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
LAUX LAWYERS AG [LLAG-2]	DSG	3		e	Antrag: Korrektur der folgenden Definitionen: **Bekanntgabe / Bekanntgeben**: Offenbaren von Personendaten an einen Dritten, der nicht Auftragsdatenbearbeiter ist. Begründung: **Für die vorgenannten, wesentlichen Begriffe, fehlen z.T. Definitionen, was in der Praxis der Digitalisierungsbestrebungen von Unternehmen teilweise zu Problemen führt.** Die Begriffe „Übermittlung", „Übertragung" und „Bekanntgabe" sollten konsequent mit unterschiedlichem Gehalt verwendet werden, wobei zusätzlich der Begriff der Offenbarung als wesentliches Abgrenzungskriterium definiert werden sollte (zur Abgrenzung zwischen code layer und content layer siehe Weber/Laux/Oertly,

					Datenpolitik als Rechtsthema, Zürich 2016, 5), wie folgt: ● Übermittlung: Übermittlung liegt vor, wenn einer der folgenden Vorgänge gemeint ist: (i) Verschiebung Daten von einem Datenträger auf einen anderen Datenträger, sei es nun ein eigener Datenträger oder ein Datenträger eines Dritten, ungeachtet des Umstands, ob ein Offenbaren resultiert (auf dem content layer) oder nicht (z.B. wenn nur verschlüsselte Daten übermittelt werden); (ii) Offenbaren von Informationen (Personendaten) an einen Dritten ausserhalb einer Datenspeicherung (blosse Einsichtnahme). Dieser Begriffsgehalt dürfte in Art. 5 und 6 VE-DSG gemeint sein. ● Übertragung: Übertragung meint den der Auftragsdatenbearbeitung vorgelagerten Vorgang, wobei nach der bisher geltenden Rechtslage keine Differenzierung vorgenommen wurde danach, ob (a) der Auftragsdatenbearbeiter nur intransparente Daten bearbeitet (d.h. im Normalbetrieb ohne Zugriff auf die Inhaltsebene, wie es z.B. für einen modern organisierten Betreiber von Rechenzentren der Fall ist) oder ob (b) der Auftragsdatenbearbeiter in einer für ihn transparenten Weise auch die Inhaltsebene (content layer) bearbeitet (wie es z.B. für einen Dienstleister der Fall ist, der eine Versicherungsgesellschaft im Underwriting unterstützt). Übertragung ist ein Unterfall der Übermittlung. ● Bekanntgabe: Bekanntgabe meint das Zugänglichmachen von Personendaten bei gleichzeitiger Offenbarung (oder Möglichkeit zur Kennntnisnahme) ohne dass ein Fall der Auftragsdatenbearbeitung gemäss Art. 7 VE-DSG (d.h. eine „Übertragung“) vorliegt. Der Begriff der Bekanntgabe wird in Art. 5 und 6 sowie in Art. 13 und 14 VE-DSG thematisiert. Bekanntgabe ist ebenfalls ein Unterfall der Übermittlung. ● Offenbaren: Einsichtnahme in den content layer von Personendaten, d.h. unter tatsächlicher Möglichkeit des Erkennens des inhaltlichen Gehalts von Personendaten (z.B. Ansicht mithilfe einer Applikation, mithilfe eines Bildschirms, oder dergleichen). Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG

LAUX LAWYERS AG [LLAG-3]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Übermittlung / Übermitteln**: Zugänglichmachen von Personendaten in Form der Bekanntgabe, der Übertragung. Eine Übermittlung liegt auch vor, wenn Personendaten in Verbindung mit Massnahmen, die eine Offenbarung ausschliessen, einem Dritten zugänglich gemacht werden. Begründung: siehe den Kommentar zu Art. 3 lit. e VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG
LAUX LAWYERS AG [LLAG-4]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Übertragung / Übertragen**: Einbezug eines Auftragsbearbeiters in die Bearbeitung von Personendaten, mit oder ohne Offenbarung der Personendaten gegenüber dem Auftragsbearbeiter. Begründung: siehe den Kommentar zu Art. 3 lit. e VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG
LAUX LAWYERS AG [LLAG-5]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Offenbarung / Offenbaren**: Ermöglichen der Einsichtnahme in die in Personendaten enthaltenen Angaben (content layer). Begründung: siehe den Kommentar zu Art. 3 lit. f VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG

LAUX LAWYERS AG [LLAG-6]	DSG	3		i	Antrag: Anpassung von Art. 3 lit. i wie folgt: *Auftragsdatenbearbeiter: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.* Begründung: Anpassung an die Begrifflichkeiten in der europäischen Gesetzgebung. Inhaltlich ist die in der EU gebräuchliche Begriffsverwendung zutreffender. Es geht beim Auftragsdatenbearbeiter nicht darum, dass er *irgendeinen* Auftrag des Verantwortlichen ausführt, sondern es geht darum, dass der Auftrag sich auf die Bearbeitung von Daten (Personendaten) bezieht. Die möglicherweise aus sprachlichen Gründen gewollte Vereinfachung ist ein unnötiges Abweichen vom EU-weiten Verständnis. Einordnung in Kürze: • Swiss Finish (nur Begriffliches)
UX LAWYERS AG [LLAG-7]	DSG	5	2		Antrag: Anpassung von Art. 5 Abs. 2 wie folgt: *Personendaten dürfen ins Ausland bekannt gegeben werden, wenn ~~der Bundesrat festgestellt hat, dass~~ die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet. Soweit der Bundesrat die Angemessenheit festgestellt hat, gilt der Nachweis für einen angemessenen Schutz ohne Weiteres als erbracht.* Begründung: Nach Art. 5 Abs. 2 in Verbindung mit Art. 5 Abs. 3 VE-DSG ist die Übermittlung von Personendaten in einen Staat, für den der Bundesrat den angemessenen Schutz (noch) nicht festgestellt hat, grundsätzlich unzulässig. Dies ist zu schablonenhaft und auch zu schwerfällig. Entscheidend ist, ob das Zielland für das konkrete Vorhaben einen angemessenen Schutz bietet (was der Verantwortliche freilich wird nachweisen müssen, wenn kein Bundesratsentscheid vorliegt). Wer einen Cloud Anbieter einsetzt, bleibt in der

					Verantwortung, aber Beweismittelbeschränkungen zum Nachweis, dass der Schutz angemessen ist, sind fehl am Platz. Der Verantwortliche sollte unter Art. 5 Abs. 3 lit. b jegliche Form von „spezifischen Garantien" nachweisen können. Die Liste des Bundessrats sollte für aufgeführte Staaten eine Positivliste sein, auf die sich der auslagerungswillige Verantwortliche verlassen dürfen. Einordnung in Kürze: • formaler Compliance-Ansatz statt risikobasierter Regelung
LAUX LAWYERS AG [LLAG-8]	DSG	5	5		Antrag: Reaktionsfrist des Beauftragten ist auf 30 Tage zu reduzieren. Begründung: Die Frist zur Genehmigung ist mit einem halben Jahr zu lange angesetzt. In Bezug auf Binding Corporate Rules (Art. 5 Abs. 3 lit. d) ist nicht einzusehen, inwiefern neu statt wie bisher 30 Tagen (Erledigungsfrist) eine (durch Nachfrage oder Beschwerdeverfahren) sich in die Länge ziehende Frist von 6 Monaten notwendig sein soll. In Bezug auf standardisierte Vertragsgarantien ist die Sechsmonatsfrist noch weniger nachvollziehbar, handelt es sich doch um Vertragsstandards, die der Beauftragte ja schon kennt (hat er sie doch selber ausgestellt, anerkannt oder genehmigt, wie Art. 5 Abs. 3 lit. c VE-DSG klarstellt). Einordnung in Kürze: • Sachfremde Regelung • Widerspricht dem Ziel, die Wettbewerbsfähigkeit der Schweiz zu stärken
LAUX LAWYERS AG [LLAG-9]	DSG	5	6		Antrag: Art. 5 Abs. 6 ist ersatzlos zu streichen. Begründung: Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert;

					die EU GDPR kennt eine entsprechende Informationspflicht auch nicht. Einordnung in Kürze: • Swiss Finish
LAUX LAWYERS AG [LLAG-10]	DSG	7	3		Antrag: Präzisierung dahingehend, dass vor Beizug von Subunternehmern nicht jeweils eine Zustimmung im Einzelfall erforderlich ist, sondern eine pauschale Genehmigung des Beizugs – wie in Art. 28 EU-GDPR – genügt. Begründung: Eine vorgängige schriftliche Zustimmung ist in der Praxis kaum umsetzbar. Die Regelung sollte analog Art. 28 Abs. 2 DSGVO ausgestaltet werden, wonach die Zustimmung zur Übertragung an einen anderen Auftragsbearbeiter in allgemeiner Form erfolgen kann, mit einem Einspruchsrecht des Verantwortlichen bei Änderungen. Dem VE-DSG ist zu Gute zu halten, dass dies wohl auch so gemeint ist und eine Abweichung zur EU-DSGVO gar nicht beabsichtigt ist. Allerdings ist die Präzisierung notwendig. Einordnung in Kürze: • Sachfremde Regelung • Widerspricht dem Ziel, die Wettbewerbsfähigkeit der Schweiz zu stärken
LAUX LAWYERS AG [LLAG-11]	DSG	12			Antrag: Streichung von Art. 12 VE-DSG. Begründung: Die Regelung ist erbrechtlicher Natur und verallgemeinert Szenarien, die sich letztlich auf die Herausgabe von Daten von Social Media Plattformen beziehen. Sie ist inhaltlich nicht notwendig. Gegebenenfalls sollte die Fragestellung in verallgemeinerter Form im Rahmen der Diskussion zum Recht auf Kopie / Recht auf Datenportabilität geführt werden.

					Einordnung in Kürze: • Relevanz im Kontext Recht auf Kopie
LAUX LAWYERS AG [LLAG-12]	DSG	13	4		Antrag: Streichung. Begründung: Die Bestimmung ist systemwidrig. Die Auftragsdatenbearbeitung basiert auf dem Konzept einer Privilegierung (der Auftragsdatenbearbeiter ist der „lange Arm“ des Verantwortlichen; alles, was der Verantwortliche darf, darf er auch durch einen Auftragsdatenbearbeiter ausführen lassen). Damit ist nur die Bekanntgabe (Übermittlung von Personendaten an Dritte ohne Bindung) datenschutzrechtlich relevant. Dieses Konzept würde mit einer Informationspflicht bei Einsetzen eines Dritten durchbrochen. Solange der Verantwortliche einen Auftragsdatenbearbeiter rechtmässig und unter Einhaltung der gesetzlich vorgeschriebenen Sicherungsmassnahmen beizieht, besteht kein Anlass für eine Information. Die Bestimmung hat neben anderen nachteiligen Wirkungen insbesondere auch **bremsenden Einfluss auf die Digitalisierung der Schweiz**, namentlich wenn es um den Einsatz von IT-Dienstleistern als Auftragsdatenbearbeiter geht: Die Möglichkeit, IT-Dienstleister – namentlich Cloud-Anbieter – beizuziehen, ist von zentraler Bedeutung (Erhöhung der Agilität und der technischen und organisatorischen Sicherheit bei einem spezialisierten Anbieter). Bereits Art. 7 Abs. 4 VE-DSG zeigt (wie das bisherige Recht), dass jedenfalls der IT-Dienstleister nicht als Dritter zu bezeichnen ist. Die (wie erwähnt) systemwidrige Einführung einer Informationspflicht im Fall einer Bearbeitung von Personendaten über einen Auftragsdatenbearbeiter (z.B. Speicherung von Daten in den Rechenzentren eines spezialisierten Anbieters) würde völlig zu Unrecht suggerieren, dass aus einer Auftragsdatenbearbeitung per se zusätzliche Risiken resultieren und umgekehrt beispielsweise der Betrieb eigener Rechenzentren (nota bene ggf. auch ohne die dazu notwendigen internen Kompetenzen) sicherer ist, als die Auslagerung dieser Aufgabe an einen spezialisierten Anbieter. Dies wäre offensichtlich falsch und somit ist Art. 13 Abs. 4 VE-DSG geradezu gegenläufig zu den Interessen der betroffenen Person (das Gesetz

					muss den Beizug von spezialisierten IT-Dienstleistern begünstigen, nicht erschweren). Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-13]	DSG	16			Antrag: Im Sinne eines Minimalantrags (aus der Optik Cloud Computing) sollte Art. 16 Abs. 1 VE-DSG wie folgt geändert werden: Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen. Begründung: Keine direkte Pflicht des Auftragsdatenbearbeiters: Nur der Verantwortliche ist hier in die Pflicht zu nehmen. Wenn auch der Auftragsdatenbearbeiter in die Pflicht genommen würde, entstünde ein direkter Widerspruch zu Art. 7 Abs. 4 VE-DSG. In eher allgemeiner Weise ist anzumerken, dass die Datenschutzfolgeabschätzung an sich obsolet wäre. Die Forderung von Art. 8bis der Konvention 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 des Vorentwurfs (Datensicherheit) bereits erfüllt. Die interne Dokumentationspflicht nach Art. 19 lit. a VE-DSG ist ausreichend. Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-14]	DSG	17	4		Antrag: Art. 17 Abs. 4 ist wie folgt neu zu formulieren: Der Auftragsdatenbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte

					Datenbearbeitung, die in der vom Auftragsdatenbearbeiter zu kontrollierenden Sphäre eintritt. Begründung: Mit Blick auf die Strafsanktion in Art. 50 Abs. 3 lit. b VE-DSG (Busse bis CHF 500'000) sind die Risikosphären zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter auch im Tatbestand von Art. 17 Abs. 4 VE-DSG abzugrenzen. Wenn auch der Auftragsdatenbearbeiter in die Pflicht genommen würde, entstünde ein direkter Widerspruch zu Art. 7 Abs. 4 VE-DSG. Ganz generell muss in Bezug auf das Institut „Data Breach Notification" angemerkt werden, dass die Blossstellungssanktion dieses Instruments systematisch zunächst nur in der US-amerikanischen Rechtsordnung sinnvoll ist (in den USA gilt ein stärker „transaktionaler", d.h. auf Transaktionen fokussierender Datenschutz, während das CH-Recht (und auch das EU-Recht) mit der Begründung von subjektiven Datenschutzansprüchen einen anderen Ansatz verfolgt). Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-15]	DSG	18	1 und 2		Antrag: Art. 18 Abs. 1 ist wie folgt neu zu formulieren: Der Verantwortliche ~~und der Auftragsbearbeiter sind~~ist verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. Art. 18 Abs. 2 ist wie folgt neu zu formulieren: Er ist~~Sie sind~~ darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind. Begründung: Mit Blick auf die Strafsanktion in Art. 51 Abs. 1 lit. e VE-DSG (Busse bis CHF 500'000) sind die

					Risikosphären zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter auch im Tatbestand von Art. 18 Abs. 1 VE-DSG abzugrenzen. Wenn auch der Auftragsdatenbearbeiter in die Pflicht genommen würde, entstünde ein direkter Widerspruch zu Art. 7 Abs. 4 VE-DSG. Der Verantwortliche hat – wie bereits Art. 7 Abs. 2 VE-DSG als Voraussetzung für eine Übertragung im Sinne von Art. 7 VE-DSG verlangt – dafür zu sorgen, dass der Auftragsdatenbearbeiter die von ihm benötigten Massnahmen zur Verfügung stellt, damit er als Verantwortlicher seinen Pflichten nach Art. 18 VE-DSG nachkommen kann. Dies hat der Auftragsdatenbearbeiter allerdings nur auf Instruktion bereitzustellen (selbstverständlich werden Cloud-Anbieter aus eigenem Antrieb solche Massnahmen bereitstellen). Inwiefern diese aber für die Zwecke des Verantwortlichen tauglich sind – und dies ist die allein relevante Frage, weil der Auftragsdatenbearbeiter die ihm zugänglich gemachten Daten ja gerade nicht zu eigenen Zwecken bearbeiten darf, wenn er die Stellung als (im Sinne von Art. 7 Abs. 4 VE-DSG privilegierter) Auftragsdatenbearbeiter nicht verlieren soll –, muss nicht der Auftragsdatenbearbeiter entscheiden; dies liegt in der Verantwortung des Cloud-Kunden, der seine Rolle als Verantwortlicher wahrzunehmen hat. Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-16]	DSG	19		b	Antrag: Art. 19 lit. b ist zu streichen, mitsamt der entsprechenden Strafbestimmung. Begründung: Nicht umsetzbar, führt zu Informationsflut. In gewissen Fällen ist die vorgesehene Informationspflicht schlichtweg sinnlos, z.B., wenn Personendaten gelöscht werden, weil sie nicht mehr benötigt werden. Einordnung in Kürze: • Praktikabilität / Sinnhaftigkeit der Regelung • Schädliche Überinformation / mehr Information resultiert nicht in mehr Datenschutz • Systemwidrig, soweit der Auftragsdatenbearbeiter verpflichtet sein soll

LAUX LAWYERS AG [LLAG-17]	DSG	20	5		Antrag: Art. 20 Abs. 5 VE-DSG ist wie folgt zu ändern: Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er die ihm vorliegenden Angaben zum Verantwortlichen nicht bekannt gibt~~, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat.~~ Begründung: Die Regelung in Art. 20 Abs. 5 Satz 2 VE-DSG ist wenig vorteilhaft für Cloud-Anbieter mit Sitz in der Schweiz. Die Regelung würde von Cloud-Anbietern mit Sitz in der Schweiz verlangen, dass sie ähnlich einer Bank ein Know Your Customer-Dossier anlegen (um den Kunden konkret identifizieren zu können). Sollten sie dies nicht tun, müssten sie Auskunft geben zu Nutzungshandlungen, zu denen sie gar nichts aussagen können (weil sie eben gemäss technischem Setup keinen Zugriff auf die Datenbearbeitungsvorgänge auf ihren IT-Infrastrukturen nehmen bzw. nicht nehmen wollen). Ad absurdum geführt: Die Regelung würde einem Cloud-Anbieter geradezu vorgeben, eben doch auf Daten des Cloud-Kunden Zugriff zu nehmen, um für den Ernstfall (Auskunftspflicht) gewappnet zu sein. Das kann nicht gewollt sein. (Pro Memoria: Gemäss Art. 50 Abs. 1 lit. a VE-DSG soll eine Verletzung der Auskunftspflicht mit Busse bis zu CHF 500'000 bestraft werden können). Mit der Regelung, dass diese Situation stets dann eintreten soll, wenn der Cloud-Kunde im Ausland seinen Sitz oder Wohnsitz hat, werden Cloud-Anbieter mit Sitz in der Schweiz und weltweitem Kundenkreis systematisch eingeschränkt. Diese Regelung verstösst klar gegen den Wunsch des Bundesrats, die Wettbewerbsfähigkeit der Schweiz zu stärken. Einordnung in Kürze: • Systemwidrige Regelung • Schwächung des Wirtschaftsstandorts Schweiz
LAUX LAWYERS	DSG	44	3		Antrag: Art. 44 Abs. 3 VE-DSG ist zu löschen.

AG [LLAG-18]					Begründung: Vorsorgliche Massnahmen im Bereich von Datenbearbeitungen können zerstörerische Konsequenzen für Unternehmen haben. Sie können einen Betrieb lahmlegen. Es sollte dem Gericht aufgrund des konkreten Einzelfalles überlassen sein zu entscheiden, die aufschiebende Wirkung zu entziehen. Da von dieser Wirkung auch geplante Cloud-Auslagerungsvorhaben betroffen sein könnten, ist diese Bestimmung auch im vorliegenden Kontext zu nennen. Einordnung in Kürze: • Unbegründeter Eingriff in das Prozessrecht
LAUX LAWYERS AG [LLAG-19]	DSG	50 ff.			Antrag: Das Sanktionenkonzept ist gesamthaft zu überdenken. Strafsanktionen gegen Individuen sind nicht vorzusehen, es sei denn, es solle ganz direkt kriminelle Energie eines Einzelnen ausserhalb seiner organisatorischen Stellung im Unternehmen z.B. des Verantwortlichen sanktioniert werden.
LAUX LAWYERS AG [LLAG-20]	DSG	59			Antrag: Art. 59 ist gesamthaft zu überdenken. Im Sinne von Bestandes- und Vertrauensschutz sind getätigte Investitionen namentlich von Cloud-Kunden zu schützen. Begründung: Bereits bestehende technische Cloud-Setups sollte ein Kunde nicht allein deswegen aufgeben müssen, weil revidierte Datenschutzgesetz in Kraft tritt. Es besteht Bedarf für angemessene Übergangsbestimmungen.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Burgdorf, 31. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt Localnet AG, Burgdorf, gerne wahr.

Die Localnet AG (Burgdorf) ist ein Anbieter von Telekommunikationsnetzinfrastrukturen und -dienstleistungen. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung

zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung" durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale

Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung

der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-Shop" nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden."). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands."[2]

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen."[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die an-

---

1 Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

2 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

3 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

wesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichenden Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80'000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365" für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei."[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40'000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10'000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5'000 – 10'000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5'000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7'500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5'000 – 30'000
Privacy by Default	1 – 40 Stunden		500 – 5'000
Betriebliche Datenschutzbeauftragter		500 – 2'000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5'000

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1'532'160'000, resp. im Durchschnitt von CHF 2'520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

„Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die

---

6 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

7 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

8 In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14'000 – 149'000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

9 608'000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

> Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen."[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

---

[10] RFA DSG, Regulierungsfolgeabschatzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (neu)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*" grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (Beispiel: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz", Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis" abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten". Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten" konsumiert. Der Begriff des „Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil" des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling" gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish" versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage" eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling" verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist" gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag" (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag" wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter").
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten" aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit" einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig", „freiwillig und eindeutig", „ausdrücklich" und die Abgrenzung zur blossen „Einwilligung" (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig", „eindeutig" oder „ausdrücklich" auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise" völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste.
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen.	**Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen.
[5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	**Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen" Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	**Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche" Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen" reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish" erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte.
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	**Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant" zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves" und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4.	
[3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten" und „Persönlichkeitsprofilen". Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat". Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet; b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist; d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. **Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert. **Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. 2 Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. 3 Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle 1 Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. 2 Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen 1 Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. 2 Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. 3 In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1" (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen. [2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen". Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen" und ersetzen mit „seine Untersuchungen". Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500'000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1'000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5'000 – 30'000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten" wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom … *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom…. *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom …… *Art. 114 Bst. f* Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …… *Art. 243 Abs. 2 Bst. d* [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 ... Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Localnet AG

Hans Rudolf Röthlisberger
Leiter Elektrizität und Kommunikation

Urs Schäppi
Leiter Kommunikation

Amstutz Jonas BJ

Von: Stefan Pfister <Stefan.Pfister@localsearch.ch>
Gesendet: Montag, 3. April 2017 16:07
An: Amstutz Jonas BJ
Cc: Guido Streit
Betreff: Stellungnahme zum Vorentwurf DSG
Anlagen: 170331 Stellungnahme localsearch_final.doc

Sehr geehrter Herr Amstutz

In der Anlage finden Sie die Stellungnahme der Swisscom Directories AG zum vor Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf).

Freundliche Grüsse

Stefan Pfister
Leiter Recht & Compliance
T +41 58 262 73 48
stefan.pfister@localsearch.ch

localsearch · Swisscom Directories AG
Förrlibuckstrasse 62 · 8021 Zürich
www.localsearch.ch

Zeigen Sie sich auf local.ch und search.ch · www.localsearch.ch
Folgen Sie uns auf Social Media · www.localsearch.ch/de/socialmedia

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swisscom Directories AG

Abkürzung der Firma / Organisation : localsearch

Adresse : Förrlibuckstrasse 60/62, 8005 Zürich

Kontaktperson : Herr Stefan Pfister, Leiter Legal & Compliance

Telefon :

E-Mail : stefan.pfister@localsearch.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	Die Swisscom Directories AG tritt unter den Markennamen local.ch, search.ch und localsearch auf. Als von der Gesetzesrevision stark betroffene Firma bedanken wir uns für die Möglichkeit zur Stellungnahme und stehen auch im Weiteren gerne für eine Mitarbeit bei der Erarbeitung zur Verfügung. Wir verweisen auf die Stellungnahme der Swisscom Schweiz AG und heben untenstehend einige Punkte hervor.
Fehler! Verweisquelle konnte nicht gefunden werden.	Insgesamt begrüssen wir die Revision des DSG und das damit angestrebte Ziel, die Angemessenheitserklärung der EU für die Schweiz aufrecht zu halten. In einigen Bereichen schiesst die Vorlage jedoch über dieses Ziel hinaus und bedarf unseres Erachtens einer Überarbeitung.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
localsearch	VE-DSG	1			Zweckbestimmung: Die Zweckbestimmung erinnert daran, dass der Datenschutz im Grundsatz den materiellen «Persönlichkeitsschutz» bezweckt. Daran hat sich der Gesetzgeber zu erinnern und möglichst auf formale Bestimmungen bzw. Verschärfungen, soweit sie zur Erreichung der Äquivalenz nicht tatsächlich notwendig sind, zu verzichten.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	2	1		Geltungsbereich: Der Verzicht auf den Schutz der Daten juristischer Personen ist grundsätzlich nachvollziehbar. Umso wichtiger wird die Einhaltung der anderen Schutzrechte juristischer Personen sein, damit diese durch die Revision nicht schlechter gestellt werden als unter geltendem Recht (vgl. Anpassung BGÖ). Der Klarheit halber wäre ein Wort (allenfalls im erläuternden Bericht) zur Behandlung der Einzelfirma wünschenswert; etwa ob eine Eintragung derselben im Handelsregister

					hier eine Auswirkung hat. Die Frage wird bei uns oft auftreten, da wir viele Einzelfirmen zu unseren Kunden zählen. Wir wünschen uns daher eine Klarstellung des rechtlichen Status (juristische oder natürliche Person) im erläuternden Bericht. Als Beispiel: Frau Heidi Huber betreibt ein kleines Coiffeurgeschäft. In unseren Verzeichnissen ist sie zunächst als Privatperson eingetragen (bspw. Heidi Huber, Adresse, Telefonnummer). Später lässt sie sich zusätzlich als «Coiffeur Heidi», Adresse, Telefonnummer eintragen.
localsearch	VE-DSG	2			Bei hängigen Verfahren soll das DSG – wie im geltenden Recht – nicht anwendbar sein.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	3		f	Begriffsbestimmung Profiling: Eine Präzisierung wäre wünschenswert in dem Sinne, dass Profiling nur vorliegt, wenn das Ergebnis einen direkten Personenbezug hat. Entgegen den Vorgaben des europäischen Rechts ist mit der jetzigen Formulierung auch das nicht-automatisierte Profiling erfasst (vgl. Art. 4 Ziff. 4 EU-DSGVO). Wir erachten daher die vorliegende Formulierung als zu weit gefasst und schlagen vor, die Begriffsbestimmung derjenigen der EU-DSGVO anzupassen und damit das nicht-automatisierte Profiling auszunehmen.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	4	6		Einwilligung: Wir begrüssen die Tatsache, dass die Einwilligung auch weiterhin durch konkludentes Handeln möglich ist (ausser bei Art. 4 Abs. 6 letzter Satz). Die verlangte ausdrückliche Einwilligung für das Profiling erachten wir aufgrund der zu umfassenden Definition des Profilings als zu weit gehend. Auch hier würde unseres Erachtens eine konkludente Einwilligung ausreichen.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	5/6			Bekanntgabe ins Ausland, allgemein: Wir erachten die Genehmigungs- und Meldepflichten als sehr weit gefasst und unpraktikabel; zumal in der Praxis der Beauftragte nicht in der Lage ist, sämtliche Verträge zu prüfen. Desweitern besteht für die Unternehmungen ein Geheimhaltungsbedarf, welcher aufgrund des Öffentlichkeitsprinzipes ausgehebelt werden kann, indem die Verträge beim Beauftragten eingesehen werden könn(t)en. Im Einzelnen siehe folgende Einträge.
localsearch	VE-DSG	5	5		Die dem Beauftragten eingeräumte Frist von sechs Monaten erachten wir als zu lang. Wir schlagen vor, die Frist auf einen Monat zu verkürzen (bisherige Frist).
localsearch	VE-DSG	6	1		Die Meldepflicht für jede Bekanntgabe der Personendaten nach Buchstaben b, c und d ist unseres

					Erachtens überschiessend und widersprüchlich. Sie geht jedenfalls weiter als die Vorgabe von Art. 12 Abs.5 E-SEV 108 (Information nur auf Antrag). Wir schlagen vor, die Meldepflicht analog zu Art. 12. Abs. 5 E-SEV 108 auszugestalten und eine Information nur auf Antrag vorzusehen.
localsearch	VE-DSG	7	2		Es erscheint nicht möglich, dass der Auftragsbearbeiter *sämtliche* Rechte der betroffenen Personen wahren kann. Gemäss dem Wortlaut wäre er aber dazu verpflichtet. Diese Bestimmung ist zu streichen bzw. auf die Gewährleistung der Datensicherheit zu reduzieren.
localsearch	VE-DSG	7	3		Auftragsdatenbearbeitung: Zu begrüssen ist, dass die schriftliche Zustimmung zur Unterauftragserteilung in Form einer allgemeinen Einverständniserklärung erfolgen kann, andernfalls wäre diese Bestimmung nicht praktikabel.
localsearch	VE-DSG	8/9			Art. 8 und 9 VE-DSG sind überschiessend (vgl. Bemerkung zu Art. 1 VE-DSG). Sie widersprechen dem Gedanken der Selbstregulierung auf welchem die EU-DSGVO (vgl. Art. 40 f.) beruht. Zudem stellt sich die Frage der Rechtsstaatlichkeit, da gegen Empfehlungen des Beauftragten kein Rechtsmittel ergriffen werden kann. Entsprechend sollten die Regelungen betr. «Good practice» analog der Regelungen der EU ausfallen.
localsearch	VE-DSG	12	3		Daten Verstorbener: Dass das Auskunftsrecht den Berufs- und Amtsgeheimnissen vorgehen soll, sollte unseres Erachtens überdacht werden. Grundsätzlich ist ausserdem zu sagen, dass die EU-DSGVO, die Schengen RL und der SEV 108 nicht auf die Daten von Verstorbenen Anwendung finden. Das Thema ist unseres Erachtens im ZGB anzusiedeln. Der Artikel ist ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	13	1/2		Wir verweisen hier auf die Stellungnahme der Swisscom.
Fehler! Verweisquelle konnte nicht	VE-DSG	13	4		Aktive Informationspflicht bei Bearbeitung durch Auftragsdatenbearbeiter ist wenig praktikabel. Wir schlagen die Streichung dieser Pflicht vor.

gefunden werden.localsearch					
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	15	2		Aktive Informationspflicht über automatisierte Einzelfallentscheidungen: Das Äusserungsrecht des Betroffenen halten wir für zu weitgehend (zur Entscheidung selbst und nicht nur zur Datengrundlage). Wir schlagen vor, das Äusserungsrecht auf die Datengrundlage zu beschränken.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	16	1		Datenschutzfolgeabschätzung: Statt von einem undefinierten «erhöhten» Risiko wäre es hier klarer, von einem «hohen» Risiko für eine Persönlichkeitsverletzung (vgl. Zweckartikel) zu sprechen.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	16	3/4		Datenschutzfolgeabschätzung: Die Meldepflicht an den Beauftragten halten wir für wirkungslos. Der Beauftragte hat eine Frist von drei Monaten, um die präsentierten Ergebnisse und Massnahmen zu beanstanden. Diese «Warte-»Frist verzögert bzw. verhindert in aller Regel die geplanten Projekte. Gleichzeitig ist nicht klar, ob nach Ablauf dieser drei Monate die Massnahmen als «genehmigt» gilt. Wir regen daher die Streichung der Meldepflicht an den Beauftragten an.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	17			Wir verweisen hierzu auf die Stellungnahme der Swisscom bzw. des VUD.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	18			Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen: Die Grundsätze Privacy by Design und Privacy by Default sind bereits heute Teil der Datensicherheit. Die Formulierung ist jedoch unklar und im Vergleich zur EU-DSGVO überschiessend. Zudem haben wir Bedenken was die dazugehörige Sanktionsnorm betrifft (siehe hinten zu Art. 51 Abs. 1 Bst. e).
localsearch	VE-DSG	19		a	Weitere Pflichten: Der Artikel wirkt insgesamt wie ein Auffangtatbestand für „übrige“ Sachverhalte. Wir verweisen hierzu im Übrigen auf die Stellungnahme der asut und des VUD.

localsearch	VE-DSG	19		b	Wir verweisen hierzu auf die Stellungnahme der Swisscom bzw. des VUD.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	20	2		Auskunftsrechte: Wie in Art. 13 wird hier eine Generalklausel mit anschliessendem Katalog eingeführt. Praktikabler wäre der abschliessende Katalog. Zudem ist die Bekämpfung des Missbrauchs der Auskunft nicht geregelt.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	20	3		Hier wäre eine Beschränkung auf die automatisierte Einzelfallentscheidung angebracht. Die Umschreibung «eine Entscheidung» ist zu unbestimmt und ausufernd.
Fehler! Verweisquelle konnte nicht gefunden werden.localsearch	VE-DSG	50 ff			Wir verweisen hierzu auf die Stellungnahme der Swisscom.

MANOR

Eidgenössisches Justiz- und
Polizeidepartement EJPD
CH-3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

4. April 2017

Vernehmlassung zum neuen Datenschutzrecht: Stellungnahme Manor

Sehr geehrte Damen und Herren

Gerne möchten wir von der Seite Manor an der Vernehmlassung für das neue Datenschutzgesetz teilnehmen. Manor ist Mitglied in der *Swiss Retail Federation* und verweist für die Detailanträge auf die Stellungnahme der Swiss Retail Federation.

Wir sind von der Revision der aktuellen Datenschutzgesetzgebung in vielfältiger Weise betroffen. Insbesondere im Bereich Kundenbindungs- und Bonusprogramme ist der Schutz von Daten ein sensibles Thema und für uns und den Schweizer Detailhandel von grosser Bedeutung.

Gerne nehmen wir wie folgt Stellung:

- **JA** zu einer grundsätzlichen Revision des Datenschutzgesetzes
- **NEIN zum vorliegenden Vorentwurf. Für den Detailhandel sind folgende Anpassungen notwendig, um die neue Datenschutzgesetzgebung unterstützen zu können:**
  - **Keine Bestimmungen, die über die EU-Regelungen hinausgehen („Swiss Finish") und die Unternehmen unnötig finanziell und administrativ belasten**
  - **Der Nutzen der Daten für den digitalen Fortschritt ist im Interesse der Konsumenten und der Unternehmen zu berücksichtigen und gegenüber dem Persönlichkeitsschutz sorgfältig abzuwägen**
  - **Keine Behinderung von Innovation und Entwicklung neuer Geschäftsmodelle**
  - **Bedarfsgerechte und konsumentenfreundliche Auskunfts- und Informationspflichten**
  - **Berücksichtigung des Prinzips der Selbstregulierung [*Good practice*-Initiativen durch (Branchen-)Verbände]**
  - **Verzicht auf strafrechtliche Sanktionen von Privatpersonen, ausser bei Absicht**

- **JA zur Übernahme der Richtlinie (EU) 2016/680** zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen
- **JA zur Revision des Übereinkommens SEV 108** zum Schutz von Menschen bei der automatischen Verarbeitung personenbezogener Daten

Im Folgenden finden Sie unsere grundsätzlichen Bemerkungen, gefolgt von den wichtigsten Kernanliegen für den Detailhandel. Im beiliegenden Formular finden Sie zudem ergänzend unsere konkreten Anträge und Bemerkungen zum Gesetzestext.

Grundsätzliche Bemerkungen

Swiss Retail begrüsst die Absicht des Bundesrats, das aktuelle Datenschutzgesetz aufgrund der neuen EU-Datenschutzgesetzgebung, welche ab 1. Mai 2018 in Kraft tritt, zu überarbeiten. Den Detailhandels-Unternehmen ist bewusst, dass eine entsprechende Angleichung der Schweizer Gesetzgebung notwendig wird, um weiterhin Daten in einem internationalen Kontext zu bearbeiten und wettbewerbsfähig zu bleiben. Die Totalrevision soll genutzt werden, um auch bestehende Bestimmungen zu hinterfragen und an die technologischen Entwicklungen anzupassen.

Die Detailhandelsbranche steht gegenwärtig unter grossem Druck und befindet sich in einem durch die Digitalisierung angetriebenen Strukturwandel. Das stationäre Geschäft wird zunehmend in den Online-Handel verlagert und die Unternehmen sind darauf angewiesen, neue Geschäftsmodelle und -strategien zu entwickeln, um die teils sinkenden Umsätze aufzufangen. **Die bessere Personalisierung von Angeboten und Angebotsinspiration wird für den Schweizer Detailhandel daher künftig überlebenswichtig sein, insbesondere, um auch im internationalen Konkurrenzkampf bestehen zu können.**

Wir möchten festhalten, dass eine Einschätzung des Vorentwurfs aufgrund der hohen Komplexität der Vorlage insgesamt schwierig ist. Der Vorentwurf lässt zahlreiche Fragen offen und es bleibt unklar, wie sich die Revisionsvorschläge auf die betrieblichen Abläufe und das wirtschaftliche Wohlergehen der betroffenen Unternehmen auswirken würden. Aus dem erläuternden Bericht geht zudem oftmals nicht klar hervor, welche Bestimmungen zwecks EU-Kompatibilität übernommen werden müssen und bei welchen Änderungen es sich um „freiwillige" Regelungen handelt. Diese Frage ist aus unserer Sicht jedoch zentral.

Grundsätzlich gilt, dass nur revidiert werden soll, was auch wirklich notwendig ist. Die EU-Kompatibilität und die Gleichwertigkeit der Schweizerischen Gesetzgebung sind sicherzustellen, aber ohne überschiessende Tendenzen und ohne einen „Swiss Finish", der über die EU-Gesetzgebung hinausgeht. Begrüssenswert ist hingegen, dass die Schweiz ihren Handlungsspielraum nutzt, wie es der Bundesrat beispielsweise im Bereich der Datenportabilität gemacht hat.

Aus Sicht des Detailhandels sind die folgenden sieben Kernanliegen zu berücksichtigen und wir beantragen, den Vorentwurf entsprechend zu überarbeiten:

1. **Datenschutz darf kein Innovationhemmnis sein und den Detailhandel als einzelne Branche nicht übermässig belasten:** Ein wichtiges Ziel der neuen Gesetzgebung muss unseres Erachtens darin bestehen, Personendaten ausreichend zu schützen, ohne dabei Innovationen auszubremsen. Der aktuelle Vorentwurf bestätigt leider unser „Gesamtunbehagen", dass der Persönlichkeitsschutz per se über die Entwicklungsmöglichkeiten der Unternehmen gestellt wird. Persönlichkeitsschutz und Mehraufwände für die Unternehmen (z.B. Aufwände für die einzuholende Information, der Auskunft oder das Einholen einer Einwilligung) müssen jedoch sorgfältig gegeneinander abgewogen und in ein adäquates Verhältnis gestellt werden. Folgeregulierungen, die nachfolgend unter Punkt 2 - 7 einzeln genannt werden, dürfen keine unverhältnismässigen Investitions- und Betriebskosten nach sich ziehen und die Unternehmen nicht unnötig belastet werden.

2. **Melde-, Auskunfts- und Informationspflichten: Verbesserung der allgemeinen und prinzipiellen Information der betroffenen Personen an Stelle einer Überinformation**

   Aus Sicht von Swiss Retail wurden die Informations-, Auskunfts-, und Meldepflichten insgesamt zu weitgehend ausgebaut und gehen teilweise deutlich über die EU Datenschutz-Grundverordnung

hinaus. Unter anderem muss sofort bei der Speicherung von Daten informiert werden und zur Informationspflicht gehört auch die Identität des Datenbearbeiters – beides sind Punkte, welche die EU Datenschutz-Grundverordnung nicht verlangt. Zudem muss jeder Datenschutzverstoss, sowohl Verletzungen von Sicherheitsbestimmungen, als auch unverhältnismässig genutzte Daten, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) gemeldet werden. Die Informationspflichten sind insgesamt schwammig und bringen eine vermehrte Rechtsunsicherheit. Gleichzeitig fallen die vorgesehenen strafrechtlichen Sanktionen streng aus. Das Ziel einer grösseren Transparenz wird unseres Erachtens nicht erreicht, indem die Unternehmen die betroffenen Personen mehr und öfters über die einzelnen Datenbearbeitungsvorgänge informieren. Wie im Detailhandel beispielsweise Erfahrungen mit Produkteinformationen zeigen, kann ein Zuviel an Informationen unter Umständen sogar kontraproduktiv sein und den Konsumenten desensibilisieren, wenn sich dieser von der Informationsflut überfordert fühlt. Aus Angst vor möglichen Sanktionen werden Unternehmen zudem lieber ein Zuviel an Informationen liefern. **Eine risikobasierte Transparenzpflicht und eine allgemeine Information der betroffenen Personen über die Folgen einer Datenpreisgabe ist unseres Erachtens weitaus zielführender. Die geplanten Meldepflichten gegenüber dem EDÖB sind wirtschaftsfreundlich und pragmatisch auszugestalten.**

Aus Sicht der Detailhandelsbranche sind entsprechend insbesondere nachfolgende Punkte zu berücksichtigen:

- **Keine Bekanntgabe von Identität und Kontaktdaten der Auftragsdatenbearbeiter, keine Informationspflicht bei indirekter Datenbeschaffung:** Art. 13 VE-DSG sieht eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister oder Kartenakzeptanzdienstleister) vor. Die Kontaktdaten der Auftragsdatenbearbeiter sollen offengelegt werden. Diese Zusatzbestimmungen sind zu streichen, denn sie gehen unseres Erachtens klar über das EU-Recht hinaus und sind weder sinnvoll noch erforderlich. In der Praxis ist es für Unternehmen damit praktisch unmöglich, Daten bei Dritten zu beschaffen, da diesen die relevanten Eckwerte (z.B. erstmalige Speicherung) oftmals gar nicht bekannt sind. Im Detailhandel werden Kundendaten häufig durch Kartenakzeptanzdienstleister oder andere Dienstleister bearbeitet. Für die Unternehmen bedeutet es insgesamt ein grosser Mehraufwand und greift zudem in berechtigte eigene Datenschutzinteressen und die Geschäftsgeheimnisse ein. Für die Kunden führt eine solche Regelung wiederum zu einer Informationsflut ohne erkennbaren Mehrwert. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist zudem bereits in Art. 7 VE-DSG geregelt.

- **Zusätzliche Massnahmen gegen missbräuchliche Auskunftsbegehren:** Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EU-DSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht generell bei Entscheidungen, die auf einer Datenbearbeitung basieren. Die kostenlose Auskunftspflicht kann zu Fehlanreizen und zu einem unverhältnismässigen Mehraufwand für die Unternehmen führen. Im neue Datenschutzgesetz sind daher Mechanismen vorzusehen, um die Unternehmen vor offensichtlich nicht datenschutzrelevanten Auskunftsbegehren zu schützen.

- **Warte- und Antwortfristen dürfen die Handlungsfähigkeit der Unternehmen nicht einschränken:** Der Bearbeitungsaufwand der Meldungen seitens der Behörde ist bereits heute gross und wird in Zukunft dank den ausgebauten Pflichten erneut zunehmen. Für Swiss Retail ist entscheidend, dass die Warte- und Antwortfristen – beispielsweise bei den unter Punkt 4 genannten Datenschutz-Folgeabschätzungen – sich auf ein sinnvolles Mass beschränken, damit die Unternehmen weiterhin handlungsfähig bleiben.

- **Keine übermässige Dokumentations- und Meldepflicht für die Unternehmen**: Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung. Diese besagt, dass *gewisse* Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen. Eine Meldung an den EDÖB sollte insgesamt nur dann erfolgen müssen, wenn nach ergriffen Schutzmassnahmen ein grosses Risiko verbleibt. Es ist klar zu regeln, welche Informationen weitergeleitet werden müssen, zudem ist die vorgesehene Reaktionszeit des EDÖB von drei Monaten auf einen Monat zu reduzieren, damit die Handlungsfähigkeit der Unternehmen gewährleistet bleibt

3. **„Profiling" ist als Erweiterung des bestehenden „Persönlichkeitsprofils" zu sehen:** Die unternommenen Anstrengungen für die Einwilligung zur Erstellung und Bearbeitung von Persönlichkeitsprofilen müssen unseres Erachtens zwingend ihre Gültigkeit behalten, auch wenn die Begrifflichkeit zu Profiling geändert wird (Vgl. Art. 4, Abs. 6. VE-DSG). In den Übergangsbestimmungen ist entsprechend klar zu regeln, dass eine „ausdrückliche Einwilligung" nur für ein neues Profiling gilt und für bereits eingeholte Daten nicht erneut das Einverständnis der betroffenen Personen eingeholt werden muss. In den bestehenden Bonus- und Kundenbindungsprogrammen unserer Mitglieder wird bei Neuanträgen beispielsweise in den Allgemeinen Geschäftsbedingungen das explizite Einverständnis der Kundinnen und Kunden für die Erstellung und Bearbeitung von Persönlichkeitsprofilen eingeholt. Ein erneutes Einholen des Einverständnisses gemäss neuem DSG wäre für all diese „alten Anträge" ein grosser Mehraufwand für die Unternehmen und würde die Weiterführung der bestehenden Bonusprogramme gefährden.
   Aus unserer Sicht unabdingbar ist, dass unter einer „ausdrücklichen Einwilligung" auch in Zukunft nicht nur ein aktives mündlich oder schriftliches Einverständnis zur Datenverarbeitung zu verstehen, sondern auch ein konklusives bejahendes Verhalten (bspw. im Rahmen von AGBs, wo betr. der Datenverarbeitung zwar nicht alleine und explizit ein Verständnis gegeben wird, aber implizit, mit Annahme der AGB).

4. **Massvolle Umsetzung der Datenschutz-Folgenabschätzung:** Das in Art. 16 VE-DSG neu eingeführte Instrument der Datenschutz-Folgeabschätzung ist aus Sicht von Swiss Retail zu weit gefasst und auf ein sinnvolles Mass zu beschränken. Die offene und unklare Formulierung führt dazu, dass in der Praxis für alle Datenbearbeitungen vorgängig aufwendige Abklärungen durchgeführt werden müssten. Verstösse würden sanktioniert, was in den Unternehmen zu einer übervorsichtigen Haltung führen und sich innovationshemmend auswirken würde. Die Datenschutz-Folgeabschätzungen und die entsprechende Informationspflicht an den EDÖB sind analog der europäischen EU-DSGVO auf Fälle zu beschränken, bei denen ein «hohes Risiko» und das Risiko einer klaren Persönlichkeitsverletzung besteht. Der Auftragsdatenbearbeiter ist von der Datenschutz-Folgenabschätzungspflicht auszunehmen, da dieser nicht über die notwendigen Angaben verfügt.

5. **Gewährleistung Rechtssicherheit:** Durch die risikobasierte, prinzipienorientierte Ausgestaltung des neuen DSG entstehen vermehrt Interpretationsspielräume und Unklarheiten. Diverse entscheidende Aspekte müssen zudem erst noch auf dem Verordnungsweg präzisiert werden. Swiss Retail fordert, dass der Gesetzgeber bei der Umsetzung (beispielsweise der „Good Practices" durch den EDÖB) auf eine klare Linie achtet. Der Vorentwurf ist auch in Bezug auf eine präzise und einheitliche Terminologie zu überarbeiten, wie beispielsweise eine klare Differenzierung zwischen „Beschaffung" und „Bearbeitung", sowie der Begriffe „Dritte" und „Empfängerinnen und Empfänger".

6. **Sanktionssystem mit Augenmass: keine strafrechtliche Sanktionierung von Privatpersonen bei Fahrlässigkeit, sondern nur bei Absicht:** Swiss Retail lehnt das im Vorentwurf skizzierte

Sanktionssystem ab. Die strafrechtlichen Sanktionen wurden im Vorentwurf insgesamt zu stark ausgebaut und fokussieren auf die mit dem Datenschutz betrauten Mitarbeitenden als Privatpersonen, anstatt auf die Unternehmen. Die geplanten Strafverschärfungen (Bussen bis 500'000.-, Freiheitsentzug bis zu 3 Jahre bei Zuwiderhandlungen) schiessen über das Ziel hinaus. Auch die vorgesehene Möglichkeit, Mitarbeitende bereits bei fahrlässigem Handeln zu bestrafen, sind nicht zielführend und untergraben den risikobasierten Ansatz, den die Revision eigentlich verfolgt. Im Detailhandel werden schützenswerte Personendaten heute zumeist in den CRM-Abteilungen von Unternehmen und vermehrt mittels automatisierter Bearbeitungsprozesse bearbeitet. Neben einer allgemeinen Kultur des gegenseitigen Denunzierens würde es zunehmend unmöglich, qualifiziertes Personal zu finden, das sich dem Risiko einer persönlichen Strafbarkeit aussetzt. Die Folge wäre ein sukzessiver Qualitätsabfall im Bereich der Datenbearbeitung.

7. **Selbstregulierung und „Empfehlungen der guten Praxis":** Swiss Retail fordert eine konsequente Umsetzung des Selbstregulierungsprinzips. Die Initiative für die in Art. 8 VE-DSG skizzierten „Empfehlungen der guten Praxis" soll von den (Branchen-)Verbänden und nicht vom EDÖB ausgehen. Das garantiert sachgerechte Lösungen, die von Experten mit einem starken Bezug zur Praxis ausgearbeitet und von den Unternehmen auch umgesetzt werden können. Auch unter der EU-DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen. Dem EDÖB ist ein Mitwirkungsrecht einzuräumen. Die „Empfehlungen der guten Praxis" sollen freiwillig bleiben, das heisst die Unternehmen halten das auch Gesetz ein, wenn sie an Stelle der Empfehlungen eigene, datenschutzkonforme Lösungen umsetzen.

Manor lehnt die Totalrevision des DSG in der vorliegenden Form, wie sie in die Vernehmlassung geschickt worden ist, ab. Die Revision enthält zahlreiche Informations- und Handlungspflichten, von welchen der Detailhandel überproportional negativ betroffen wäre. Dies hätte zur Folge, dass die Kosten im Detailhandel zusätzlich steigen und die Unternehmen belasten. Die anfallenden Kosten würden nicht zuletzt indirekt an die Konsumentinnen und Konsumenten überwälzt, was nicht der Sinn der Revision sein kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und einer entsprechenden Überarbeitung des Vorentwurfs. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Beat Flury
Leiter Wirtschaftspolitik Manor AG

Amstutz Jonas BJ

Von: Füzesséry-Minelli Simone
Gesendet: Montag, 3. April 2017 10:56
An: Perler Cornelia BJ
Betreff: TR: STN Mastercard
Anlagen: communication-confirmation.pdf

-----Ursprüngliche Nachricht-----
Von: _BJ-Eingabe
Gesendet: Freitag, 31. März 2017 17:35
An: Perler Cornelia BJ <Cornelia.Perler@bj.admin.ch>
Betreff: WG: OSIS-BV - FOJ - 8c9d8cfc-9b23-4866-97e1-67ad91a1eaea - 2017-03-31 17:31:03 (YYYY-MM-DD, CE(S)T)

-----Ursprüngliche Nachricht-----
Von: osis-bj@e-service.admin.ch [mailto:osis-bj@e-service.admin.ch]
Gesendet: Freitag, 31. März 2017 17:31
An: _BJ-Eingabe <eingabe@bj.admin.ch>
Betreff: OSIS-BV - FOJ - 8c9d8cfc-9b23-4866-97e1-67ad91a1eaea - 2017-03-31 17:31:03 (YYYY-MM-DD, CE(S)T)

Einfache Eingabe / Demande simple / Richiesta semplice / Simple submission

an/à/a/to: Federal Office of Justice; Bundesrain 20; CH-3003 Bern
Einheit/Unité/Unità/Unit: General inbox

E-Mail-Adresse des Absenders / Adresse de courriel de l'expéditeur / Indirizzo e-mail dello speditore / Sender's e-mail address:
caroline.louveaux@mastercard.com; No account on a delivery platform

Betreff / Concerne / Oggetto / Subject:
Avant-Projet LPD / commentaires de Mastercard

Please refer to the contents of the submission in the attached communication-confirmation.pdf document and any attachments.

OSIS-BV System (Open eGov Secure Inbox Service) https://www.e-service.admin.ch/wiki/display/openegovdoc/OSIS-BV

Einfache Eingabe / Quittung **Demande simple / Reçu** **Richiesta simplice / Ricevuta** **Communication / Receipt**	Digitally signed by Open eGov Secure Inbox Service Bern - Switzerland, 2017-03-31 Reception confirmed

Empfänger Destinataire Destinatario Recipient	Federal Office of Justice Bundesrain 20 CH-3003 Bern
Einheit / Kontaktperson Unité / Personne de contact Unità / Persona di contatto Unit / Person	General inbox --/--
Eingangsdatum / ID Data de réception / ID Data ricezione / ID Reception date / ID	2017-03-31 17:31:03 (YYYY-MM-DD, CE(S)T) 8c9d8cfc-9b23-4866-97e1-67ad91a1eaea
Aktenzeichen / Betreff Référence / Concerne Riferimento / Oggetto Reference / Subject	--/-- Avant-Projet LPD / commentaires de Mastercard
Mitteilung Message Communicazione Communication	Bonjour, Vous trouverez ci-joint les commentaires de Mastercard sur l'avant-projet de révision de la LPD. N'hésitez pas à nous contacter si vous avez des questions ou si vous souhaitez en discuter. Nous restons à votre entière disposition. Bien à vous, Caroline Louveaux
Beilagen Annexes Allegati Attachments Hashes (SHA-256)	**The documents sent as attachments/enclosures are displayed in the attachment window of the original Adobe Reader. If you cannot open a document by double-clicking on it, drag it onto the desktop or into a folder and open it there.** **Die als Beilagen/Anlagen übermittelten Dokumente werden im Anlagen-Fenster des Original Adobe Reader angezeigt. Falls Sie ein Dokument nicht durch Doppelklicken öffnen können, ziehen Sie es auf den Desktop oder in einen Ordner und öffnen Sie es dort.**
	Mastercard - commentaires - 31 mars 2017.pdf b4fab4c96871e451eaa52b2b0decd8837624a117c858e17504352c11952da026
Identität des Senders Identité de l'expéditeur Identitàdel mittente Identity Sender	--/--
Kontaktinformationen Coordonnées de l'expéditeur Dettagli di contatto Contact details	Mastercard Mrs Caroline Louveaux 198A chaussée de Tervuren 1410 Waterloo Belgium T: +32 498585205
E-Mail / Zustellplattform Courriel / Plateforme de messagerie E-Mail / Piataforme di consegna E-Mail / Data exchange platform	caroline.louveaux@mastercard.com No account on a delivery platform
Antwort Réponse Risposta Answer	Unencrypted to the above e-mail address

Code / Codice	247582

Le 31 mars 2017

AVANT-PROJET DE REVISION DE LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES EN SUISSE – COMMENTAIRES DE LA SOCIETE MASTERCARD

Mastercard est une entreprise globale de paiement et de technologie qui opère un réseau de paiement électronique au nom et pour le compte de ses clients, à savoir les institutions financières établies en Suisse et partout dans le monde. Nous accueillons favorablement le projet de révision de la loi fédérale sur la protection des données du 19 juin 1992 (« LPD »), en ce qu'il donne l'opportunité d'assurer une protection plus adaptée des droits des individus dans le contexte de l'économie digitale, ainsi que de mettre un place un régime proportionné et cohérent pour les entreprises actives sur le continent européen. Nous sommes particulièrement intéressés par un rapprochement encore plus significatif entre les législations de l'Union européenne et de la Suisse en matière de protection des données, et donc par un rapprochement entre la LPD et le nouveau règlement général européen sur la protection des données (« GDPR »).

L'avant-projet de révision de la LPD (« Projet de loi ») contient des éléments très positifs et montrent d'ores et déjà des pistes intéressantes d'un rapprochement cohérent avec le GDPR. Néanmoins, nous avons repéré certains éléments du Projet de loi qui méritent une réflexion plus approfondie ainsi que des clarifications et modifications pour conjuguer la protection des individus et les intérêts légitimes des entreprises traitant leurs données.

Pour chaque thème, nous suggérons des pistes de réflexions et de modification qui nous semblent appropriées dans le cadre d'une plus grande cohérence entre droit suisse et droit européen de la protection des données. Les ajouts de mots sont **sous-lignés** et les mots supprimés sont ~~**rayés**~~.

Le 31 mars 2017

Résumé des suggestions de modification du Projet de loi.

1. *Champ d'application*: Préciser que le Projet de loi porte sur les données personnelles.

2. *Profilage - atteinte à la personnalité – décision individuelle automatisée*:
   - Clarifier la définition de profilage et supprimer la référence au profilage à l'Article 4§6;
   - Supprimer les « activités sans le consentement exprès de la personne concernées » de la définition de l'atteinte à la personnalité (ou tout du moins préciser que cette définition vise spécifiquement les décisions individuelles automatisées produisant des effets juridiques concernant une personne ou l'affectant de manière significative) ;
   - Ajouter comme motif justificatif « le traitement de données personnelles nécessaire à des fins d'amélioration de la sécurité, de la prévention et de la détection de la fraude et autre atteinte sévère pour la personne concernée ou d'autres personnes »;
   - Préciser que le droit de recevoir des informations sur le résultat d'une décision, la manière dont elle a été obtenue et ses conséquences ne s'applique qu'aux décisions prises exclusivement sur base d'un traitement automatisé de données produisant des effets juridiques concernant une personne ou l'affectant de manière significative.

3. *Sous-traitance :*
   - Préciser que le sous-traitant peut se baser sur l'accord écrit préalable général ou spécifique du responsable du traitement pour l'utilisation de tiers ;
   - Limiter l'information des personnes concernées en cas d'utilisation de sous-traitant aux catégories de sous-traitants utilisés ;
   - Ne pas imposer au sous-traitant de répondre à une demande d'accès.

4. *Analyse d'impact relative à la vie privée :* Introduire des éléments de la *risk-based approach* dans le mécanisme d'analyse d'impact relative à la vie privée ; en particulier, limiter la communication des résultats de l'analyse d'impact au préposé aux situations où le risque accru pour la personnalité et les droits fondamentaux de la personne concernée persiste malgré la mise en place de mesures visant à diminuer le risque.

5. *Sécurité des données personnelles :* Introduire des éléments de la *risk-based approach* dans l'obligation sécuriser les données.

6. *Notification des violations de données personnelles:* Préciser les conditions, modalités et exemptions relatives à l'obligation de notifier les violations de données personnelles au préposé et/ou aux personnes concernées.

7. *Obligations dites de privacy by design et privacy by default :* Préciser que les mesures de *privacy by design* et *privacy by default* doivent prendre en compte en particulier l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, relatifs au traitement.

I. Champ d'application

- ***Suggestion***.

  Article 1 : La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données **personnelles** font l'objet d'un traitement.

  Article 2§1 : La présente loi régit le traitement de données **personnelles** concernant des personnes physiques effectué par (a) des personnes privées ; et (b) des organes fédéraux.

- ***Justification***. Le Projet de loi se doit d'être extrêmement clair quant à l'objectif qu'il poursuit. Cet objectif est inscrit à l'Article 1 du Projet de loi indique que celui-ci « vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données font l'objet d'un traitement ».

  De même, l'Article 2 paragraphe 1 précise que le Projet de loi précise le champ d'application du Projet de loi, à savoir « le traitement de données concernant les personnes physiques effectué par des personnes privées et des organes fédéraux ».

  Ces deux dispositions très importantes dans le Projet de loi ne précisent pas que les « données » auxquelles elles font référence sont des données personnelles, telles que définies à l'Article 3(a). Or, il est important que les dispositions concernant l'objectif et le champ d'application du Projet de loi soient très claires quant au type de données auquel s'applique le Projet de loi. Les Articles 1 et 2 du GDPR indiquent par ailleurs explicitement que cette législation s'applique au traitement de données personnelles. Nous suggérons donc de **préciser que le Projet de loi régit uniquement le traitement de données personnelles**.

II. Profilage - Atteintes à la Personnalité – Décisions Individuelles Automatisées

Le Projet de loi remplace la définition de « profil de la personnalité » par la définition du « profilage » dans son Article 3. L'utilisation de la notion de « profilage » se retrouve également dans le GDPR. Un tel rapprochement des législations de l'UE et de la Suisse apporterait plus de sécurité juridique pour les entreprises respectant les législations européenne et suisse en matière de protection des données personnelles et serait donc très appréciable.

Néanmoins, certaines dispositions du Projet de loi n'assurent pas un niveau de clarté et de sécurité juridiques suffisants. Le texte actuel du Projet de loi crée en effet un risque de confusion entre différents concepts que sont le profilage et les données sensibles, dont découlent des obligations peu adaptées ou disproportionnées pour les responsables de traitement. Nous examinons plus en détails ces dispositions en (A) et (B) ci-après.

A. Définition du profilage

- ***Suggestion***.

Article 3 (f) : Profilage : toute exploitation de données personnelles ~~**ou non**~~, consistant à analyser ou prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime, ou ses déplacements.

- ***Justification***. Le profilage est un type de traitement défini à l'Article 3(f) comme « toute exploitation de données personnelles ou non, consistant à analyser ou prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime, ou ses déplacements ». De nombreux types de traitements utilisant des données non personnelles risquent d'être capturés par cette définition. Il existe ici un risque de confusion entre traitements de données personnelles et non personnelles, alors même que le champ d'application du Projet de loi est la protection des données personnelles uniquement. Il existe également un risque d'insécurité juridique accru par rapport à la définition du profilage dans le GDPR qui se limite au traitement de données personnelles. Pour ces raisons, **nous recommandons de limiter la définition de profilage à l'Article 3(f) à la seule exploitation de données personnelles** consistant à analyser ou prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime, ou ses déplacements.

B. Principes relatifs au profilage

Le Projet de loi prévoit plusieurs dispositions qui nécessitent d'être alignées avec les principes du GDPR car elles créent un risque de confusion entre données sensibles et profilage et imposent des obligations disproportionnées aux responsables de traitement utilisant le profilage dans des situations comportant peu de risques pour les droits et libertés des individus.

1. <u>Consentement exprès en cas de profilage</u>

- ***Suggestion***.

Article 4 §6 : Lorsque son consentement est requis pour justifier le traitement de données personnelles, la personne concernée ne consent valablement que si elle exprime sa volonté librement, clairement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles~~**, ou en cas de profilage,**~~ son consentement doit être au surplus exprès.

- ***Justification***. L'Article 4§6 prévoit l'obligation d'obtenir le consentement exprès de l'individu en cas de traitement de données sensibles ou de profilage. Le GDPR prévoit cette même obligation concernant le traitement de données sensibles uniquement, qui requièrent bien évidemment une protection particulière compte tenu des risques pour les droits et libertés des individus lorsque des données comme les données de santé ou d'appartenance religieuse sont en jeu par exemple. Néanmoins, cette disposition crée un amalgame entre les données sensibles qui comportent un risque plus important pour les droits des individus par nature, et les activités de profilage qui ne comportent pas nécessairement de risques plus importants qu'un autre type de traitement de données

personnelles. Il faut noter ici que le GDPR n'indique en aucune façon que le profilage est une activité « sensible ». Ce sont les décisions fondées exclusivement sur un traitement automatisé (y compris le profilage) qui sont soumises à un régime spécifique dans le GDPR, non le profilage en tant que tel. Nous recommandons dès lors de **supprimer la référence au profilage de l'Article 4§6** pour une meilleure clarté et sécurité juridiques pour les nombreuses entreprises soumises au droit suisse et européen de la protection des données personnelles.

2. Atteinte à la personnalité et motifs justificatifs

- ***Suggestion***.

  - Option A pour l'Article 23 §2 (d): ~~**faire du profilage sans le consentement exprès de la personne concernées**~~.

    ou

  - Option B pour l'Article 23 §2 (d) : ~~**faire du profilage**~~ **prendre des décisions individuelles produisant des effets juridiques concernant une personne ou l'affectant de manière significative et prises exclusivement sur la base d'un traitement automatisé** sans le consentement exprès de la personne concernées **ou sans un des motifs justificatifs listés à l'Article 24**.

    ET

  - Article 24§2 : (Nouveau) **g. les données personnelles sont traitées à des fins d'amélioration de la sécurité, de prévention et de la détection de la fraude et autre atteinte grave pour la personne concernées ou d'autres personnes.**

- ***Justification***. L'Article 23 §2(d) inclut les activités de profilage sans consentement exprès de l'individu concerné dans la définition d'une atteinte à la personnalité. Cette disposition découle manifestement de l'Article 4§6. L'Article 23§2(d) renforce l'amalgame entre données sensibles et profilage. Or, le profilage n'a pas pour objectif ni ne conduit automatiquement à des atteintes à la personnalité. Certaines activités de profilage basées sur le traitement de données personnelles ont même des retombées positives pour les individus ainsi que pour la société. Par exemple, la lutte contre la fraude est capitale pour assurer la stabilité financière des systèmes de paiement, et dès lors pour renforcer la confiance des citoyens dans l'économie digitale, dans l'intérêt de tous. Il faut noter ici que la lutte contre la fraude tient une place spécifique dans le GDPR dont le considérant 47 permet aux responsables de traitement de traiter des données pour cette finalité sur la base de ses intérêts légitimes (qui sont analysés en tenant compte des intérêts des individus concernés), sans le consentement des individus. Nous recommandons dès lors de **supprimer dans la définition de l'atteinte à la personnalité les activités de « profilage sans le consentement exprès de la personne concernée » à l'Article 23 §2(d)** (voir Option A ci-dessus)**.** Si par cas l'Article 23§2(d) devait être

conservé dans le Projet de loi, nous suggérons de le **modifier afin que celui-ci vise spécifiquement les décisions individuelles automatisées produisant des effets juridiques concernant une personne ou l'affectant de manière significative**, prises sans le consentement exprès de la personne concernée ou un autre motif justificatif prévu à l'Article 24§2 du Projet de loi (voir Option B ci-dessus).

Dans la même optique, nous recommandons de **clarifier l'Article 24§2 en ajoutant à la liste de motifs justificatifs le traitement de données personnelles nécessaire à des fins d'amélioration de la sécurité, de la prévention et de la détection de la fraude et autre atteinte sévère pour la personne concernée ou d'autres personnes**. Cette clarification permettrait non seulement d'aligner la LPD avec le GDPR mais surtout de maintenir les activités de lutte contre la fraude qui sont essentielles à l'économie digitale et bénéfiques pour tous, y compris pour les individus eux-mêmes.

3. Demande d'accès en cas de décision individuelle automatisée

- ***Suggestion***.

  Article 20§3 : Lorsque le traitement de données personnelles conduit à une ~~**décision, en particulier à une décision individuelle automatisée,**~~ **décision ayant des effets juridiques sur la personne concernée ou qui l'affecte de manière significative et qui est prise exclusivement sur la base d'un traitement automatisé,** la personne concernée reçoit des informations sur le résultat de la décision, la manière dont elle est obtenue ainsi que sur ces conséquences.

- ***Justification***. L'Article 20§3 semble être en rapport avec les décisions ayant des effets juridiques sur la personne concernée ou qui l'affectent de manière significative et qui sont prises exclusivement sur la base d'un traitement automatisé. Par souci de clarté, nous recommandons de **modifier l'Article 20§3 du Project de loi pour que le droit de recevoir des informations sur le résultat d'une décision, la manière dont elle a été obtenue et ses conséquences ne s'applique qu'aux décisions prises exclusivement sur base d'un traitement automatisé de données produisant des effets juridiques concernant une personne ou l'affectant de manière significative, et non à toute décision**.

III. Sous-Traitance

Le Projet de loi incorpore différentes obligations applicables dans le contexte de la sous-traitance et du recours à des tiers par les sous-traitants. Certaines de ces obligations nécessitent des précisions et modifications afin de les rendre à la fois pratiques pour les entreprises et protectrices pour les personnes concernées.

A. Accord écrit préalable de tiers par le responsable du traitement

- ***Suggestion***.

  Article 7 §3 : Le sous-traitant peut lui-même sous-traiter un traitement à un tiers qu'avec l'accord écrit préalable**, général ou spécifique,** du responsable du traitement.

- ***Justification***. L'Article 7§3 du Projet de loi impose l'accord écrit préalable du responsable de traitement lorsque le sous-traitant sous-traite les données à un tiers. Cette disposition vise à s'assurer que le responsable de traitement garde un certain contrôle sur le traitement des données en cas de transfert ultérieur par le sous-traitant à un tiers car le responsable de traitement est l'entité principalement responsable de la conformité du traitement avec la législation en matière de données personnelles et n'a pas de relation directe avec ce tiers.

  Néanmoins, les sous-traitants ont régulièrement recours à des tiers dont les services nécessitent un accès à tout ou partie des données personnelles que le sous-traitant traite pour le compte du responsable du traitement. Ces tiers offrent des services très divers et leurs activités impliquant des données personnelles sont parfois minimes en fonction des services proposés aux sous-traitants, par exemple en cas de simples services d'hébergement des données sans manipulation particulière de ces données. De plus, certains sous-traitants peuvent utiliser plusieurs tiers selon les besoins liés au service fourni au responsable de traitement. Par ailleurs, certains sous-traitants utilisent les mêmes tiers pour fournir des services à des milliers de responsables de traitement. Pour prendre en compte ces multiples situations, il apparait important d'apporter plus de flexibilité aux responsables de traitement et sous-traitants en leur permettant utiliser un accord écrit préalable général ou spécifique. Nous recommandons dès lors de **préciser à l'Article 7§3 du Projet de loi que le sous-traitant doit obtenir un accord écrit préalable, général ou spécifique afin de sous-traiter un traitement à un tiers,** en ligne avec l'Article 28(4) du GDPR.

B. Informer les personnes concernées de l'identité et coordonnées des sous-traitants.

- ***Suggestion***.

  Article 13 §4 : Lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement ~~**communique à la personne concernée son identité et ses coordonnées, ainsi que les données personnelles ou les catégories de données personnelles concernées**~~ **informe les personnes concernées des catégories de sous-traitants concernés par ce traitement**.

- ***Justification***. Article 13§4 du Projet de loi impose au responsable de traitement d'informer les individus de l'identité et des coordonnées de son ou ses sous-traitant(s). Nous comprenons que l'Article 13 vise généralement à assurer un degré important de transparence de la part du responsable de traitement vis-à-vis des individus en ce qui concerne la façon dont leurs données personnelles sont collectées, traitées mais également partagées avec d'autres entités.

  Néanmoins, en pratique, cette obligation va nécessiter que les responsables de traitement mettent à jour très régulièrement la liste des sous-traitants et leurs coordonnées dans leurs politiques de confidentialité. Cette obligation risque de demander des efforts considérables aux entreprises sans pour autant apporter plus de protection aux individus. Au contraire, cette obligation va alourdir et complexifier les politiques de confidentialité pour les individus, ce qui risque d'aboutir à davantage de confusion plutôt que de la transparence. Nous recommandons donc de **modifier l'Article 13§4 afin**

d'imposer aux responsables de traitement l'obligation d'informer les individus de l'utilisation de certaines *catégories* de sous-traitants sans pour autant demander à ce que cette information contienne l'identité, les coordonnées, ou encore les particularités du traitement de données offerts par le sous-traitant.

C. Demande d'accès

- ***Suggestion***.

  Article 20 §5 : Le responsable du traitement qui fait traiter des données personnelles par un sous-traitant demeure tenu de fournir les renseignements demandés. ~~**Cette obligation incombe toutefois au sous-traitant, s'il ne révèle pas l'identité du responsable du traitement ou si ce dernier n'a pas de domicile en Suisse.**~~

- ***Justification***. L'obligation pour le sous-traitant de répondre aux demandes d'accès des individus s'il ne révèle pas l'identité du responsable ou si le responsable n'a pas de domicile en Suisse (Article 20§5) n'est pas assez claire et pourrait être interprétée comme une obligation quasi systématique pour les sous-traitants de répondre aux demandes d'accès à la place des responsables de traitement. Nous recommandons de **supprimer la seconde phrase de l'Article 20§5 concernant les demandes d'accès** auxquelles devront répondre eux-mêmes les sous-traitants.

IV. Analyse d'Impact Relative à la Protection des Données

- ***Suggestion***.

  Article 16:

  1. Lorsque le traitement envisagé est susceptible d'entrainer un risque accru pour la personnalité et les droits fondamentaux de la personne concernée**, et compte tenu de la nature, la portée, le contexte et les finalités du traitement,** le responsable de traitement ~~**ou le sous-traitant**~~ procède au préalable à une analyse d'impact.
  2. L'analyse d'impact expose le traitement envisagé, les risques pour la personnalité et les droits fondamentaux de la personne concernée ainsi que les mesures prévues pour réduire ces risques.
  3. **Lorsque le responsable de traitement a mis en place des mesures visant à diminuer la probabilité et gravité des risques encourus par les individus mais que le risque accru persiste malgré ces mesures,** le responsable de traitement ~~**ou le sous-traitant**~~ communique les résultats de l'analyse d'impact au préposé, ainsi que les mesures ~~**envisagées**~~ **mises en place**.
  4. Si le préposé a des objections concernant les mesures envisagées, il en informe le responsable du traitement ~~**ou le sous-traitant**~~ dans un délai de trois mois dès la réception de toutes les informations nécessaires.

- ***Justification***. L'Article 16§1 du Projet de loi demande aux responsable de traitement ou sous-traitants de procéder à une analyse d'impact relative à la protection des données (« AIPD ») préalablement à tout traitement envisagé qui est susceptible d'entrainer un risque accru pour la personnalité et les droits fondamentaux des individus. Les résultats de l'AIPD ainsi que les mesures prévues pour réduire ce risque doivent ensuite être communiqués au préposé. Cette obligation n'est pas sans rappeler la *risk-based approach* qui est la clef de voûte du GDPR. L'AIPD permet ainsi de responsabiliser les entreprises pour qu'elles prennent en compte les caractéristiques de leurs traitements de données et prennent les mesures correctives et/ou de sécurité appropriées pour réduire les risques pour les droits et libertés des individus, et de simplifier les formalités et obligations administratives pour les entreprises. Nous recommandons cependant de **préciser à l'Article 16§1 que l'existence d'un risque accru pour la personnalité et les droits fondamentaux des individus doit être évalué par le responsable de traitement en tenant compte de la nature, la portée, le contexte et les finalités du traitement envisagé.** C'est le contexte qui va généralement permettre de déterminer si un traitement présente un risque accru ou non. Telle est également l'approche adoptée à l'Article 35 du GDPR.

  Nous proposons également de **limiter les obligations de l'Article 16 du Projet de loi aux seuls responsables de traitement** tel que prévu à l'Article 35 du GDPR. Ceci se justifie par le fait que les traitements sont pensés et définis par les responsables de traitement.

  Par ailleurs, l'obligation établie à l'Article 16§3 de communiquer au préposé chaque résultat d'une AIPD ainsi que les mesures prises pour limiter les risques semble disproportionnée. En effet, lorsqu'une entreprise effectue une AIPD, elle va bien souvent identifier les risques liés au traitement envisagé et pouvoir élaborer des mesures appropriées pour limiter voire supprimer ces risques. Imposer une obligation générale de communication risque non seulement d'entraver l'innovation au vu des obligations excessives pour les entreprises, mais également d'aboutir à un engorgement du préposé. Nous recommandons de **préciser à l'Article 16§3 que cette obligation s'applique uniquement aux cas où le responsable de traitement a mis en place des mesures visant à diminuer la probabilité et gravité des risques encourus par les individus mais que le risque accru persiste malgré ces mesures**.

V. Sécurité des données personnelles

- ***Suggestion***.

  Article 11 :

  ~~Les~~ **Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour la personnalité et les droits fondamentaux des personnes concernées, les** responsables du traitement et les sous-traitants doivent assurer la sécurité des données personnelles~~. Celles-ci doivent être protégées contre tout traitement non autorisé et toute perte, par~~ **en mettant en œuvre** des mesures organisationnelles et techniques appropriées.

- ***Justification***. L'Article 11 instaure une obligation de sécurité des données personnelles contre tout traitement non autorisé ou perte de données. Cette formulation n'est cependant pas assez précise pour permettre aux responsables du traitement et sous-traitants de mieux comprendre ce qu'il faut protéger et ce qu'ils doivent prendre en considération pour aboutir à des mesures « appropriées ». Nous suggérons ici de reprendre des éléments de l'Article 32 du GDPR permettant d'**introduire une référence à la *risk-based approach* dans l'obligation de sécurité des données.**

VI. Notification des violations de la protection des données

- ***Suggestion***.

  - Article 3 :
    (Nouveau) **j. violation de données personnelles : violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la communication non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.**

  - Article 17 « Notification des violations ~~**de la protection**~~ des données **personnelles** »:
    1. Le responsable de traitement notifie ~~**sans délai au préposé tout traitement non autorisé ou toute perte de données personnelles**~~ **dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance toute violation de données personnelles**, à moins que la violation ne présente vraisemblablement pas de risques pour la personnalité et les droits fondamentaux de la personne concernée. **Le responsable de traitement est considéré comme avoir pris connaissance d'une violation de données personnelles lorsqu'il est en possession d'éléments tangibles indiquant une forte probabilité de violation.**
    2. **La notification visée au paragraphe 1 doit:**
       a. **Décrire la nature de la violation de données personnelles y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données personnelles concernées ;**
       b. **Communiquer le nom et les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenue par le préposé ;**
       c. **Décrire les conséquences probables de la violation de données personnelles :**
       d. **Décrire les mesures prises ou que le responsable de traitement propose de prendre pour remédier à la violation de données personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.**
    3. Il informe par ailleurs la personne concernée lorsque ~~**cela est nécessaire à sa protection**~~ **la violation est susceptible d'entrainer des risques accrus pour la personnalité et les droits fondamentaux de la personne concernée** ou lorsque que le préposé l'exige.
    4. Le responsable du traitement peut, dans les cas visés à l'art. 14, al. 3 et 4, restreindre la notification à la personne concernée, la différer ou y renoncer.

5. **La communication à la personne concernée visée au paragraphe 3 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :**
    a. **Le responsable de traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données personnelles affectées par ladite violation, en particulier les mesures qui rendent les données personnelles incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;**
    b. **Le responsable de traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour la personnalité et les droits fondamentaux des personnes concernées visé au paragraphe 3 n'est plus susceptible de se matérialiser ;**
    c. **Elle exigerait des efforts disproportionnés.**
6. Le sous-traitant informe sans délai le responsable du traitement de ~~**tout traitement non autorisé**~~ **toute violation** de données personnelles.

- Article 19 :
  Le responsable de traitement et le sous-traitant sont en outre tenus :
    a. De documenter leurs traitements de données personnelles ;
    b. D'informer les destinataires auxquels des données ont été communiquées de toute rectification, effacement, ou destruction des données personnelles, de toute violation ~~**de la protection**~~ des données **personnelles**, ainsi que de toute limitation du traitement selon l'art. 25, al. 2 ou art. 34 al. 2, à moins qu'une telle information s'avère impossible ou exige des efforts disproportionnés.

- Article 50 §2 :
  e. ne notifie pas au préposé les violations ~~**de la protection**~~ des données **personnelles** selon l'art. 17, al. 1.

- Article 50 §3 :
  b. n'informe pas le responsable du traitement des violations ~~**de la protection**~~ des données **personnelles** selon l'art. 17, al. ~~**1**~~**6.**

- ***Justification***. L'Article 17 du Projet de loi prévoit une obligation de notifier sans délai les violations de protection des données au préposé à moins que la violation ne présente vraisemblablement pas de risques pour la personnalité et les droits fondamentaux des individus. Cette notification doit également être faite aux individus concernés si ceci est nécessaire pour leur protection ou sur demande du préposé. Cette disposition va dans le sens d'une protection et d'objectifs de transparence accrus en faveur des individus qui est également prévue par le GDPR.

  Néanmoins, la notion de « violation de la protection des données » telle qu'elle est utilisée à l'Article 17 prête à confusion en ce qu'une « violation de la protection des données » peut être perçue comme une situation de non-conformité à loi de manière générale. Or, l'Article 17 porte plus précisément sur les situations où la sécurité des données personnelles est compromise. Nous recommandons donc

de **remplacer « violation de la protection des données » par « violation des données personnelles » à l'Article 17 du Projet de loi** pour éviter toute confusion et reprendre le langage utilisé dans le GDPR (voir la définition de la violation de données personnelles à l'Article 4§12 du GDPR). Par souci de cohérence, nous suggérons également de remplacer **« violation de la protection des données » par « violation des données personnelles» aux Articles 19, 50§2 et 50§3 du Projet de loi.**

L'Article 17 manque également de clarté quant aux aspects pratiques de ces notifications pour les entreprises. En particulier, l'immédiateté de la notification d'une violation va poser des problèmes pratiques car les entreprises ont besoin de faire remonter les informations concernant les problèmes informatiques et de les analyser pour déterminer s'il y a effectivement une violation de données, ce qui demande du temps. De même, l'appréciation du caractère « nécessaire » ou non de la notification aux individus concernés n'est pas assez clair pour les entreprises. Comme celles-ci vont devoir investir des moyens importants et créer des procédures internes pour se mettre en conformité avec les dispositions du GDPR relatives à la notification des violations de données personnelles, **il serait approprié d'aligner l'Article 17 du Projet de loi avec les Articles 33 et 34 du GDPR qui poursuivent tous le même objectif.**

VII. Protection des données dès la conception et par défaut

- ***Suggestion***.

  Article 18:

  1. Dès la conception du traitement, le responsable du traitement ~~**et le sous-traitant**~~ sont tenus de prendre les mesures appropriées pour minimiser les risques d'atteinte à la personnalité et aux droits fondamentaux de la personne concernée, et pour prévenir ces atteintes.
  2. ~~**Ils sont**~~ **Le responsable de traitement est** au surplus tenus, par le biais de préréglages appropriés, de garantir que, par défaut, seules les données personnelles nécessaires à la finalité du traitement sont traitées.
  3. **Les mesures et préréglages appropriés visés aux paragraphes 1 et 2 doivent être prises en tenant compte en particulier de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, relatifs au traitement.**

- ***Justification***. L'Article 18 prévoit une obligation dite de *privacy by design* and *privacy by default*. Cette obligation consiste à prendre en compte, dès la conception d'un traitement, les mesures appropriées pour minimiser les risques d'atteinte à la personnalité et droits fondamentaux de la personne concernée, et pour prévenir ces atteintes. Il s'agit de plus d'utiliser des réglages appropriés afin de garantir par défaut que seules les données personnelles nécessaires à la finalité du traitement sont traitées. Ces obligations sont similaires à celles de l'Article 25 du GDPR mais nécessitent certains ajustements afin de ne pas imposer un régime standardisé trop stricte aux entreprises. Il s'agit de prendre en compte le contexte dans lequel le nouveau traitement est envisagé, notamment l'état de

la technique, des coûts mais encore la nature, la portée, les finalités du traitement et la probabilité et gravité des risques présentés par ce traitement.

Nous proposons également de **limiter les obligations de l'Article 18 du Projet de loi aux seuls responsables de traitement** tel que prévu à l'Article 35 du GDPR. Ceci se justifie par le fait que les traitements sont pensés et définis par les responsables de traitement.

Nous suggérons ainsi de **modifier l'Article 18** du Projet de loi pour le rapprocher du texte de l'Article 25 du GDPR et notamment de **préciser que les mesures appropriées doivent être prises en tenant compte en particulier de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, relatifs à ce traitement.**

Amstutz Jonas BJ

Von: Katrina Riva <katrina.riva@hausaerzteschweiz.ch>
Gesendet: Freitag, 31. März 2017 14:05
An: Amstutz Jonas BJ
Cc: 'Christine Zemp'; Reto Wiesli
Betreff: mfe_révision totale de la loi sur la protection des données
Anlagen: mfe_Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de_def.doc; mfe_Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de_def.pdf

Cher Monsieur Amstutz,

Vous trouverez ci-joint la position de mfe Médecins de famille et de l'enfance Suisse relative à la révision totale de la loi sur la protection des données.
Nous vous remercions de l'opportunité qui nous a été donnée de nous exprimer sur ce sujet.

En cas de questions, nous nous tenons à votre disposition.

Avec mes meilleures salutations,

Katrina Riva-Schyrr
Collaboratrice scientifique

MEDECINS DE FAMILLE ET DE L'ENFANCE SUISSE / HAUS- UND KINDERÄRZTE SCHWEIZ
Effingerstrasse 2
CH-3011 Berne
phone 031 508 36 07
fax 031 508 36 01

mfe Haus- und Kinderärzte Schweiz
Médecins de famille et de l'enfance Suisse
Medici di famiglia e dell'infanzia Svizzera

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : mfe Haus- und Kinderärzte Schweiz

Abkürzung der Firma / Organisation : mfe

Adresse : Effingerstrasse 2, 3011 Bern

Kontaktperson : Christine Zemp Gsponer, Rechtsanwältin, Luzern

Telefon : 041 410 81 87

E-Mail : christine.zemp@swanlex.ch

Datum : 29.03.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
mfe	Das Bestreben nach einer Stärkung des Datenschutzes für die Betroffenen ist grundsätzlich zu begrüssen, ebenso die Weiterentwicklung des Datenschutzgesetzes zur Anpassung an die technologischen und gesellschaftlichen Entwicklungen. Es muss allerdings darauf geachtet werden, dass nicht über das Ziel hinaus geschossen wird, was insbesondere bei den Sanktionen von Verletzungen gilt. Zudem ist zu verhindern, dass den Ärzten und Ärztinnen durch die Gesetzesrevision weiterer administrativer Mehraufwand entsteht, der bekanntlich tariflich in keiner Weise entschädigt wird. Ein Teil der Änderungen betrifft redaktionelle Präzisierungen gegenüber dem geltenden Recht. Darauf wird nachfolgend nicht Stellung genommen. Zudem ergeben sich gewisse Änderungen aufgrund der Revision von internationalen Rechtsnormen. Zu erwähnen ist dabei das revidierte Übereinkommen des Europarates SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten, welches einen Mindeststandard vorsieht und von der Schweiz auch in der revidierten Form wieder ratifiziert werden soll. Zudem wurden die EU-Verordnung 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und die EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts (Bestandteil der Schengen-/Dublin-Regulierungen) von der EU verabschiedet. Es ist undiskutabel, dass die schweizerische Gesetzgebung den Anforderungen im europäischen Raum entsprechen muss und die Schweiz ihre Gesetze diesbezüglich anzupassen hat. Soweit sie dazu nicht rechtlich verpflichtet ist (im Zusammenhang mit dem Schengen-/Dublin-Abkommen bestehen rechtliche Verpflichtungen), drängt sich die Anpassung zur Sicherung des grenzübergreifenden Geschäftsverkehrs und somit auch aus wirtschaftlichen Interessen der Schweiz auf. Die Stossrichtung der Revision wird von mfe unterstützt. Entsprechend den nachfolgenden Ausführungen sind bei der aktuellen Vorlage noch gewisse Änderungen vorzunehmen. Dabei ist in besonderem Mass darauf zu achten, dass bei den einer Schweigepflicht unterstehenden Personen keine Friktionen zwischen den Pflichten nach DSG und nach anderen gesetzlichen Vorschriften entstehen. Dies gilt einerseits für die Strafbestimmungen (Art. 321 StGB und Art. 50 ff. DSG), aber auch für weiteren beruflichen Pflichten wie beispielsweise die Aufbewahrungspflicht.

Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
mfe	VE-DSG	3	c	3-4	*„Die folgenden Ausdrücke bedeuten: …* *c. besonders schützenswerte Daten: …* *Ziff. 3 genetische Daten,* *Ziff. 4 biometrische Daten, die eine natürliche Person eindeutig identifizieren.“* Es ist zu begrüssen, dass unter den besonders schützenswerten Personendaten neu auch die genetischen und biometrischen Daten, mit welchen eine Person eindeutig identifiziert werden kann, ausdrücklich erwähnt werden. Die Umschreibung erscheint uns korrekt.
mfe	VE-DSG	4	4		*„Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es erfordert.“* Die Pflicht zur Aufbewahrung von Personendaten kann sich nicht nur aus dem Zweck der Bearbeitung, sondern aus anderen Vorschriften, beispielsweise aus den Berufspflichten ergeben. Die meisten kantonalen Gesundheitsgesetze sehen beispielsweise die Pflicht zur Aufzeichnung und Aufbewahrung während zehn Jahren vor. Dokumente im Laborbereich und für Blut und Blutprodukte haben gar längere Aufbewahrungsfristen. Deshalb ist in Art. 4 Abs. 4 der Vorbehalt von gesetzlichen Vorschriften aufzunehmen, welche die Aufbewahrung konkret regeln.
mfe	VE-DSG	6	1	d	*„In Abweichung von Art. 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: …* *d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritte zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.“*

					Es ist zu begrüssen, dass dieser Ausnahmefall ausdrücklich Eingang ins Gesetz findet. Da ein medizinischer Notfall vorliegen muss, kann der Entscheid, ob im konkreten Fall eine Bekanntgabe zulässig ist, den Ärzten überlassen werden. Dies im Gegensatz zur Bekanntgabe der Daten eines Verstorbenen gemäss Art. 12 (sh. nachfolgend). Der Schutz des Betroffenen ist durch die Mitteilung gemäss Abs. 2 gewährleistet.
Fehler! Verweisquelle konnte nicht gefunden werden.	VE-DSSG	8			Die Empfehlungen der guten Praxis, zu erlassen in erster Linie durch den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend Beauftragten), sind ein neues Instrument. Nachvollziehbar ist, dass ein Bedürfnis besteht, die gesetzlichen Vorschriften zu konkretisieren und den Branchenbedürfnissen anzupassen. Dass auch die einzelnen Branchen („interessierten Kreise") selber Empfehlungen ausarbeiten und vom Beauftragten genehmigen lassen können, entspricht diesem Konzept. Allerdings darf nicht übersehen werden, dass diese Empfehlungen zwar grundsätzlich unverbindlich sein sollen, ihnen jedoch in der Praxis eine erhebliche Bedeutung zukommen wird. Das im Gesetz enthaltene Verfahren (*„Er zieht die interessierten Kreise bei …")* reicht aus diesem Grund rechtsstaatlich nicht aus. Es ist im Gegenteil ein formelles Recht auf Wahrung des rechtlichen Gehörs der betroffenen Kreise vorzusehen. Zudem sollen sich auch interessierte Kreise, die vom Beauftragten nicht in ein Anhörungsverfahren einbezogen werden, zu einem in Bearbeitung stehenden Thema unaufgefordert äussern können und ein formelles Recht haben, dass diese Äusserungen vom Beauftragten berücksichtigt werden. Nur so kann gewährleistet werden, dass die Interessen sämtlicher davon Betroffenen rechtzeitig in die Empfehlungen einfliessen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VE-DSSG	12			Art. 12 regelt die Einsichtnahme in die Daten einer verstorbenen Person. Dabei werden die Voraussetzungen für die Einsichtnahme umschrieben. Die Aufnahme dieses Regelungsbereichs ins Gesetz (vorher befand er sich in der Verordnung zum Datenschutzgesetz) ist zu begrüssen. Allerdings wird in Abs. 3 neu vorgesehen, dass ein allfälliges Amts- oder Berufsgeheimnis nicht geltend gemacht werden kann, wenn die Voraussetzungen für die Einsichtnahme nach Art. 12 vorliegen.

					Diese Regelung widerspricht Art. 321 StGB. Unklar ist, ob das Datenschutzgesetz neu dem Strafgesetzbuch vorgehen soll. Wenn dies der Fall wäre, würde das bedeuten, dass bei einer entsprechenden Anfrage nicht mehr eine Entbindung vom Berufsgeheimnis einzuholen wäre. Die Interessenabwägung müsste damit in jedem Fall vom Geheimnisträger selber vorgenommen werden, ohne dass er sich bei der Aufsichtsbehörde rückversichern könnte. Daraus entsteht das latente Risiko, dass sich ein Ermessensentscheid rückblickend als falsch erweist, was zu empfindlichen Sanktionen für die Auskunft erteilende Person führen kann. Für den ärztlichen Alltag kann sich die Bestimmung in dieser Form als heikel erweisen. Denn Anfragen über die Herausgabe von Daten einer verstorbenen Person haben bekanntlich oft den Zweck der Verfolgung berechtigter oder unberechtigter eigener Interessen. Es kann nicht die Aufgabe eines Arztes sein, in der ihm zur Verfügung stehenden Zeit vertiefte Interessensabklärungen zu treffen. Der Vorbehalt des Berufsgeheimnisses ist daher auch im Zusammenhang mit der Einsichtnahme in Daten von Verstorbenen weiterhin vorzusehen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VE-DSSG	20	1		Das Auskunftsrecht ist grundsätzlich kostenlos. Während in der bisherigen Fassung des Artikels über das Auskunftsrecht vorgesehen war, dass der Bundesrat die Ausnahmen regelt, enthält der Vorentwurf diese Möglichkeit nicht mehr. Gemäss Art. 2 der VO DSG kann unter anderem dann eine angemessene Kostenbeteiligung verlangt werden, wenn die Auskunftserteilung mit einem besonders grossen Arbeitsaufwand verbunden ist, wobei die Kostenbeteiligung max. CHF 300.00 beträgt. Der Bundesrat soll auch weiterhin Ausnahmen von der Kostenlosigkeit vorsehen können, weshalb Art 20, 1. Absatz entsprechend zu ergänzen ist. Dies ist gerade in Fällen wichtig, wo Fotokopien von Dokumenten zur Herausgabe erstellt werden müssen, die (noch) nicht elektronisch vorhanden sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	VE-DSSG	50-51			**Übertretungen (Art. 50 und 51):** Der Vorentwurf DSG sieht generell eine massive Erhöhung der möglichen Bussen vor, von bisher CHF 10‘000.00 (106 Abs. 1 StGB) auf bis zu CHF 500‘000.00 bei vorsätzlicher Tatbegehung bzw. bis CHF 250‘000.00 bei fahrlässiger Tatbegehung. Dagegen ist grundsätzlich nichts einzuwenden. Allerdings muss zwischen vorsätzlicher und fahrlässiger Tatbegehung stärker unterschieden werden, indem die mögliche Bussenhöhe bei Fahrlässigkeit tiefer angesetzt wird (unter CHF 250‘000.00). Eine mögliche Busse bis zu CHF 250'000.00 ist für fahrlässige Delikte zu hoch.

Fehler! Verweisquelle konnte nicht gefunden werden.	VE-DSSG	52			Der neue Art. 52 DGS soll Artikel 321 StGB für Berufe, die kein Berufsgeheimnis habe, ergänzen. Das ist sinnvoll. Unklar ist jedoch der Titel dieser Norm, soll sie doch gerade auch auf Personen Anwendung finden, die keine explizite berufliche Schweigepflicht haben. Diese Bezeichnung der Norm ist daher nochmals zu prüfen. Wichtig ist, dass die Strafandrohungen von Art. 321 StGB und Art. 52 DSG identisch geregelt sind, ansonsten die Gefahr einer ungleichen Behandlung der verschiedenen Geheimnisträger bestehen würde. Im vorgelegten Entwurf ist das der Fall.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	**Bemerkung/Anregung**

Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Migros-Genossenschafts-Bund

Eidgenössisches Justiz- und Polizeidepartement EJPD
3003 Bern

Per Mail an jonas.amstutz@bj.admin.ch

Ort/Datum Zürich, 4. April 2017

Betreff **Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)**

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Wir danken Ihnen, dass Sie uns die Möglichkeit einer Stellungnahme zum Vorentwurf zum Bundesgesetzes über die Totalrevision des Datenschutzgesetzes (VE-DSG) einräumen.

Zu den einzelnen Bestimmungen des DSG verweisen wir auf die detailliérten Erläuterungen im beiliegenden Formular.

Als Kernanliegen erachten wir folgende Themenbereiche. Wir erlauben uns, in der Folge darauf gesondert einzugehen:

1. Einleitende Bemerkungen

Die Migros als traditionsreiches und verantwortungsbewusstes Unternehmen anerkennt die Wichtigkeit des Datenschutzes und erachtet ein klares und angemessenes Datenschutzgesetz als auch für die Wirtschaft essenziell. Die Migros als grösste Detailhändlerin der Schweiz ist auf vielfältige Weise mit der Thematik des Datenschutzes konfrontiert und begegnet dieser Thematik bereits seit vielen Jahren - u.a. mit dem erfolgreichen Kundenbindungsprogramm „Cumulus" - auf sehr verantwortungsbewusste Art und Weise.

In einer zunehmend digitalen Welt ist die Akzeptanz des Nutzers und das Vertrauen in dessen verantwortungsbewussten Umgang mit den Daten eine wichtige Voraussetzung zur Erschliessung und Ausschöpfung dieses wirtschaftlichen Potenzials. Dies kann nur mit einem klaren Regelwerk erfolgen, welches sowohl die legitimen Ansprüche des Nutzers auf Wahrung seiner Persönlichkeitsrechte als auch die wirtschaftlich sinnvollen Möglichkeiten der Unternehmen berücksichtigt.

Migros-Genossenschafts-Bund
Wirtschaftspolitik
Limmatstrasse 152
Postfach 1766
CH-8031 Zürich

Direktwahl +41 44 277 25 75
Zentrale +41 44 277 21 16
Fax +41 44 277 20 09
juerg.maurer@mgb.ch
www.migros.ch

Aus Sicht der Migros sind daher der Datenschutz und die Persönlichkeitsrechte der natürlichen Personen sehr wichtig. Gleichzeitig ist aber auch darauf zu achten, dass die unternehmerische Freiheit nicht unnötig eingeschränkt wird und dass das neue Gesetz wirtschaftsfreundlich und unbürokratisch ausgestaltet wird. Fakt ist, dass für den Detailhandel neben dem Warenfluss der Datenfluss immer wichtiger und bedeutender wird. Der einheimische Detailhandel, der wegen der Frankenstärke und wegen des Einkaufstourismus unter starkem wirtschaftlichem Druck steht, darf nicht durch zusätzliche Kosten und bürokratischen Aufwand belastet werden.

2. Internationaler Kontext

Viele Schweizer Unternehmen sind heute international tätig oder bearbeiten Daten in einem internationalen Kontext. Damit ist die europäische Datenschutzgrundverordnung (DSGVO) für viele Unternehmen in jedem Fall anwendbar. Das neue DSG muss deshalb grundsätzlich gleichwertig ausgestaltet werden. Überschiessende Regeln würden hohen Zusatzaufwand verursachen und sind zu vermeiden.

Dabei gilt es aber auch, den von der DSGVO gegebenen Handlungsspielraum auszunutzen. Dort, wo praktikablere oder liberalere Regeln im Schweizer Kontext sinnvoll und der Sache dienlich sind, sind solche Regeln vorzusehen. Die Angemessenheit des Schweizer Datenschutzrechts wird dadurch keineswegs in Frage gestellt.

3. Informations- und Meldepflichten

Aus Sicht der Migros wird das Ziel einer grösseren Transparenz für die Konsumentinnen und Konsumenten verfehlt, wenn ihnen öfters und immer mehr Informationen zu einzelnen Datenbearbeitungsvorgängen zur Verfügung gestellt werden. Dies führt vielmehr zu einer Flut von Informationen und Meldungen, die es erschweren, die wichtigen Informationen vom Unwesentlichen zu unterscheiden. Zusätzlich ist von einem unverhältnismässigen Aufwand für das Unternehmen auszugehen, welcher sich innovations- und wettbewerbsbehindernd auswirken kann.

Die vorgesehenen weitgehenden Meldepflichten würden des Weiteren zur Offenlegung von Geschäftsgeheimnissen und zur Pflicht führen, sich selber zu belasten. Beides ist klar abzulehnen. Auch bei den Meldepflichten ist dem Grundsatz des risikobasierten Ansatzes in vernünftiger Art und Weise nachzukommen: Die Themenbereiche automatisierter Einzelfallentscheid, Datenschutz-Folgeabschätzung und Meldung von Datenschutzvorstössen sind entsprechend anzupassen.

4. Selbstregulierung

Der Grundsatz der Selbstregulierung wird ausdrücklich begrüsst. Allerdings ist strikte darauf zu achten, dass die Initiative für die Empfehlungen stets zwingend von den Branchen/Unternehmen selbst ausgeht. Ausdrücklich abgelehnt wird seitens Migros die Möglichkeit des Beauftragten, Empfehlungen in Eigenregie zu erlassen. Dies widerspricht dem Grundsatz der Selbstregulierung.

5. Sanktionen

Der neue Entwurf sieht einen sehr langen Strafenkatalog mit u.a. Bussen bis 500'000 Franken vor. Die Strafen zielen grundsätzlich auf natürliche Personen ab, d.h. Mitarbeitende könnten auch bei einer fahrlässigen Begehung ausgesprochen hart bestraft werden.

Die Migros lehnt die vorgesehenen Strafbestimmungen ab. Sie führen zu einer Kriminalisierung der mit dem Datenschutz betrauten Mitarbeitenden. Das ist nicht gerechtfertigt, setzt Fehlanreize und führt dazu, dass die gesetzlich gegebenen Spielräume bei der Datenbearbeitung aus Angst vor persönlicher Bestrafung nicht ausgenutzt werden. Auch wird ein Denunziantentum innerhalb der Unternehmen gefördert.

Die Sanktion ist deshalb (wie dies auch in der EU üblich ist) gegenüber dem Unternehmen auszusprechen. Dabei ist darauf zu achten, dass die Sanktion zwar wirksam und abschreckend aber auch angemessen ist.

6. Profiling

Der Begriff des Profiling ersetzt den altrechtlichen Begriff des Persönlichkeitsprofiles. Allerdings geht der Begriff viel weiter: Es wird darunter jede Auswertung von Daten verstanden, selbst wenn es sich nicht um eigentliche Personendaten handelt. Die Migros fordert, dass dieser Begriff eng zu fassen ist und bereits in der Gesetzesvorlage klar umschrieben wird.

7. Auftragsbearbeiter

In der heutigen Zeit ist es unumgänglich, bei der Verarbeitung von Daten Dritte, sogenannte Auftragsbearbeiter beizuziehen. Gemäss Entwurf müsste der Verantwortliche die betroffenen Personen immer über die Identität und die Kontaktdaten des Auftragsbearbeiters informieren. Die Migros lehnt diese Bestimmung ab, da dies zu einem grossen administrativen Mehraufwand ohne wirklichen Nutzen für die betroffene Person führen würde.

8. Daten-Folgeabschätzung; Meldung bei Datenschutzverstössen

Mit diesem neuen Instrument müsste der Verantwortliche in Fällen, welche zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, eine sogenannte Daten-Folgeabschätzung durchführen und dem EDÖB vorlegen. Diese Massnahme erachten wir als unverhältnismässig und zu bürokratisch.

Ebenfalls zu verzichten ist auf die Pflicht, dem EDÖB jeden Verstoss gegen den Datenschutz zu melden. Dadurch wird auch das straf- und verfassungsrechtliche Verbot der Selbstbelastung (nemo tenetur) verletzt. Die Meldepflicht ist auf Verletzungen der Datensicherheit zu beschränken, die eine Vielzahl von Personen betrifft.

Migros-Genossenschafts-Bund

Wir danken Ihnen für die Berücksichtigung unserer Argumente und stehen Ihnen für allfällige Rückfragen jederzeit zur Verfügung.

Freundliche Grüsse
Migros-Genossenschafts-Bund

Jürg Maurer
Stv. Leiter Direktion Wirtschaftspolitik

Dr. Ivo Caviezel
Direktion Legal und Compliance

Beilage: erwähnt

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Migros-Genossenschafts-Bund

Abkürzung der Firma / Organisation : MGB

Adresse : Limmatstrasse 152

Kontaktperson : Dr. Ivo Caviezel (Direktion Legal & Compliance)

Telefon : 044 277 21 11

E-Mail : ivo.caviezel@mgb.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
MGB	Der MGB ist sich bewusst, dass der schweizerische Gesetzgeber Vorgaben des Europarates und bis zu einem gewissen Grad auch der EU einzuhalten hat. Die europäische Datenschutz-Grundverordnung (DSGVO) verlangt allerdings keine pauschale Übernahme. Für die Angemessenheitserklärung genügt es vielmehr, grundlegende Garantien einzuhalten. Das künftige DSG sollte sich daher an der ERK 108 orientieren. Eine Verschärfung gegenüber der DSGVO ("Swiss Finish") ist erst recht abzulehnen. Ein Swiss Finish würde die schweizerischen Unternehmen benachteiligen und ihre Innovationskraft beeinträchtigen, ohne zu besserem Datenschutz zu führen. Das widerspräche u.a. der Strategie des Bundesrats für eine digitale Schweiz, die u.a. die Innovationskraft der schweizerischen Volkswirtschaft stärken möchte.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
MGB	DSG	1	2		Bei hängigen Verfahren soll das DSG – wie im geltenden Recht – nicht anwendbar sein.
MGB	DSG	3			Personendaten sind nur mehr Daten von natürlichen Personen, die Daten juristischer Personen sind vom Geltungsbereich des DSG ausgenommen. Diese Anpassung wird ausdrücklich begrüsst. Genetische Daten und biometrische Daten sollten nur dann zu besonders schützenswerten Daten zählen, wenn sie es nicht nur erlauben, sondern den Zweck haben, eine natürliche Person zu identifizieren. Dass sie es erlauben, eine Person zu identifizieren, ist nicht genug; sonst wäre jedes Foto erfasst. Der Begriff des „Profilings“ ist zu weit. Nach dem VE-DSG liegt ein Profiling • nicht nur bei einer automatisierten, sondern bei jeder Auswertung von Daten vor, und • sogar dann, wenn Daten ausgewertet werden, die gar keine Personendaten sind. Der Einbezug von anderen (nicht personenbezogenen) Daten ist abzulehnen: • Wenn jede Auswertung von Daten zu den erfassten Zwecken als Profiling gilt, dann muss wohl für jede manuelle Durchsicht von Daten eine ausdrückliche Einwilligung eingeholt werden. Das ist praktisch unmöglich. • Die Ausweitung auf eine Bearbeitung anderer Daten ist überflüssig: Die Definition der Personendaten erfasst auch Daten, bei denen die betroffene Person bestimmbar ist. Die Bearbeitung von Sachdaten ist deshalb ohnehin erfasst, wenn sie durch die Profilierung einer bestimmten Person zugeordnet wird. • Andererseits führt der Einbezug anderer Daten zu praktischen Problemen. Es stellt sich beispielsweise die Frage, ob und wenn ja wann eine ausdrückliche Einwilligung eingeholt werden muss, wenn beispielsweise Geodaten ausgewertet und diese erst später der betroffenen Person

					zugeordnet werden. Der Begriff des Profilings sollte daher analog zur DSGVO nur die automatisierte Auswertung von Daten umfassen und nur die Auswertung von Personendaten.
MGB	DSG	4	3		Das Erfordernis der "klaren" Erkennbarkeit ist zu streichen, da seine Bedeutung nicht klar ist.
MGB	DSG	4	6		Neu schreibt das DSG vor, dass eine Einwilligung eindeutig zu erfolgen hat. Was dies bedeutet, ist unklar. Die Frage der Eindeutigkeit einer Willenserklärung ist aber bereits durch das bestehende Recht geregelt. Davon sollte nicht abgewichen werden. Das Eindeutigkeitserfordernis ist daher zu streichen. Ferner sind die Ausführungen der Erläuterungen zum Vorentwurf hinsichtlich der Frage der Ausdrücklichkeit nicht klar. Sie sollten geklärt werden. Schliesslich rechtfertigt sich das Erfordernis der Ausdrücklichkeit für ein **Profiling** nicht. Der Begriff des Profiling ist zwar "gefühlt" etwas Bedrohliches. Der Begriff erfasst in der Mehrheit aber harmlose Alltagshandlungen.
MGB	DSG	5	2 und 3		Nach Art. 5 Abs. 2 und 3 ist die Übermittlung in einen Staat stets nur mit besonderen Garantien oder ausnahmsweise zulässig, wenn der betreffende Staat nicht auf der Liste des Bundesrats figuriert. Bei der Nachführung der Liste werden Verzögerungen und Fehler aber nicht zu vermeiden sein. Der Nachweis, dass ein Land ausserhalb dieser Liste dennoch angemessenen Schutz bietet, sollte deshalb offenbleiben. Mit Bezug auf nicht aufgeführte Staaten sollte die Liste daher nur eine Vermutung und keine Fiktion begründen.
MGB	DSG	5	5		Die Frist von sechs Monaten (Abs. 5), die zudem durch die Nachforderung von Informationen durch den EDÖB beliebig verlängerbar ist, macht ein Genehmigungsverfahren äussert unpraktikabel und führt zu unzumutbaren Verzögerungen bei Auslandstransfers. Eine Frist von 30 Tagen sollte genügen; sie tat es bisher auch.
MGB	DSG	5	6		Art. 5 Abs. 6 ist zu streichen. Die pauschale Informationspflicht bietet keinen Mehrwert, und die DSGVO kennt eine entsprechende Informationspflicht auch nicht (Art. 5 Abs. 6).

MGB	DSG	6	1	a	„Einzelfall“ impliziert eine allzu starke Einschränkung. Nach allgemeinen Grundregeln genügt es, wenn sich die Einwilligung auf bestimmte wiederkehrende Sachverhalte bezieht. „Im Einzelfall“ ist deshalb zu streichen.
MGB	DSG	6		b	Die Bearbeitung im Zusammenhang mit Verträgen sollte wie in der DSGVO auch Datenbearbeitungen erfassen, die lediglich im Interesse der betroffenen Person abgeschlossen werden, und Bearbeitungen von Personen, die sonstwie in die Vertragsabwicklung involviert sind (z.B. Kontaktpersonen). Die Meldepflicht von Datentransfers gestützt auf Abs. 1 Bst. b, c und d geht viel zu weit und ist nicht sinnvoll. Der EDÖB wird zudem nicht über die Kapazitäten verfügen, diese Meldungen zu bearbeiten. Diese Bestimmung sollte daher gestrichen werden.
MGB	DSG	6	2		Die Verpflichtung, den EDÖB trotz Ausnahmetatbestand zu informieren, ist unverhältnismässig und nicht praktikabel, da Ausnahmetatbestände i.d.R. zeitkritisch sind. Zudem würde diese breite Pflicht zu einer unverhältnismässig grossen Anzahl Meldungen führen. Schliesslich würde der EDÖB über heikle Verfahren und (Geschäfts-)Geheimnisse informiert, ohne dass ein (datenschutzrechtlicher) Grund dafür vorliegt. Auch ist diese Pflicht dem EU-Recht fremd. Abs. 2 ist deshalb zu streichen.
MGB	DSG	7			Bei der Verteilung der Pflichten auf den Auftragsbearbeiter und den Verantwortlichen ist kein Konzept zu erkennen. Dies sollte geklärt werden. An vielen Stellen ist es unpassend, neben dem Verantwortlichen auch den Auftragsbearbeiter in die Pflicht zu nehmen, da letzterer nur nach Weisung des Verantwortlichen handeln darf. Der Verantwortliche muss sich neu vergewissern, dass der Auftragsbearbeiter nicht nur die Datensicherheit, sondern als auch die Rechte der betroffenen Person gewährleisten kann (Art. 7 Abs. 2 VE-DSG). Es ist unklar, um welche Rechte es geht und welche Pflichten dem Auftragsbearbeiter damit überbunden werden sollen. Zudem kann der Auftragsbearbeiter nicht sämtliche Rechte der betroffenen Personen gewährleisten. Diese Bestimmung ist daher zu streichen bzw. auf die Gewährleistung der Datensicherheit zu beschränken. Zudem sollte festgehalten werden, dass die in Art. 7 Abs. 2 geforderte Vergewisserung dadurch erfolgen kann, dass der Auftragsbearbeiter über eine entsprechende Zertifizierung verfügt.

MGB	DSG	7	4		Das Schriftformerfordernis für die Zustimmung zur Übertragung der Datenbearbeitung auf einen Unter-Auftragsbearbeiter ist praxisfremd. Es genügt, eine dokumentierte Zustimmung zu verlangen. Die Zustimmung muss zudem in genereller Weise vorab möglich sein. Falls die generelle Zustimmung nur mit einem Veto- Recht des Verantwortlichen akzeptiert werden soll, ist das im Gesetz festzuhalten.
MGB	DSG	8 und 9			Der Ansatz der Selbstregulierung ist besonders bei Regulierungen wichtig, die zwar einen starken Technikbezug aufweisen, die aber dennoch wie der VE-DSG – zu Recht – technikneutral sind. Art. 8 und 9 VE-DSG werden deshalb im Grundsatz ausdrücklich begrüsst. Sie weisen im Einzelnen aber einige Mängel auf: • Im Gegensatz zu den Regelungen in der DSGVO (Art. 40 und 41), nach der eine Ausarbeitung von Verhaltensregeln nur durch Verbände und andere Vereinigungen vorgesehen ist, kann nach dem VE-DSG auch der EDÖB selbst solche Empfehlungen ausarbeiten. Dies widerspricht dem Zweck der Selbstregulierung. Zudem besteht das Risiko, dass der EDÖB das Mittel von „Empfehlungen der guten Praxis“ dazu nutzt, seiner eigenen Interpretation datenschutzrechtlicher Fragen mehr Gewicht zu verleihen. Die „Empfehlungen der guten Praxis“ sollten daher nur von den Verantwortlichen ausgehen (und allenfalls durch den EDÖB genehmigt) werden. • Die Rechtswirkungen sind zudem unklar. Es ist davon auszugehen, dass bei Einhaltung der Empfehlungen eine gesetzliche Vermutung der Gesetzeskonformität verhält. Dies sollte ausdrücklich so geregelt werden.
MGB	DSG	13			Die Informationspflicht wird auf alle Personendaten ausgeweitet. Das würde zu erheblichem Mehraufwand führen. Wir sind daher der Meinung, dass eine aktive Informationspflicht wie im heutigen Recht nur bei besonders schützenswerten Personendaten und im Fall der Profilierung bestehen sollte. In den Erläuterungen sollte ferner präzisiert werden, dass bei Änderungen keine Nachinformation erfolgen muss. Wichtig ist ferner, dass die aktive Informationspflicht ausschliesslich bei der Beschaffung gilt, nicht bei jeder weiteren Bearbeitung und auch nicht bei weiteren Bekanntgaben an Dritte. So ist Art. 13 VE-DSG auch zu verstehen, wie sich aus Abs. 1 ergibt. Die Botschaft sollte das klar festhalten. Sodann ist festzuhalten, dass die Informationspflicht in allgemeiner Weise und in standardisierter Form erfolgen kann, bspw. durch Angaben in AGB oder in einer Datenschutzerklärung auf einer Internetseite.

					Art. 13 Abs. 4 VE-DSG geht weit über die DSGVO hinaus. Diese Vorschrift würde auch zu noch umfangreicheren Informationen und dadurch mehr Aufwand und einer Überflutung mit Informationen führen. Diese Bestimmung ist zu streichen.
MGB	DSG	14			Die Berufung auf ein überwiegendes privates Interesse ist weiterhin nicht möglich, wenn die Daten einem Dritten weitergegeben werden (was z.B. auch eine Konzerngesellschaft sein kann). Diese Einschränkung sollte gestrichen werden. Sie würde besonders in Konzernverhältnisse zu einem enormen administrativen Mehraufwand führen, der in der Sache aber nicht mehr Transparenz bringt. Die Fälle, in denen ein überwiegendes privates Interesse in der Regel besteht, sollten analog zu Art. 24 VE-DSG aufgeführt werden (vgl. die Ausführungen zum Auskunftsrecht).
MGB	DSG	15			Durch Automatisierung lassen sich Effizienzgewinne und Aufwandreduktionen erzielen. Automatisierte Entscheide bringen zudem auch für Kunden grosse Vorteile (Objektivität der Entscheidung, geringere Kosten, schnellere Prozesse). Es ist deshalb falsch, die Automatisierung von Entscheiden so stark zu belasten. Art. 15 VE-DSG ist daher angemessen einzuschränken. Zunächst muss die Informationspflicht nach Art. 15 VE-DSG erfüllt werden, wenn die automatisierte Einzelentscheidung rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat. Art. 15 VE-DSG unterscheidet sich damit von Art. 22 DSGVO und Art. 8 Abs. 1 Bst. a der E-SEV 108: Bei beiden Bestimmungen wird klar, dass die Pflichten des Verantwortlichen nur greifen, wenn die Auswirkungen der automatisierten Entscheidung erheblich sind. Der Wortlaut von Art. 15 VE-DSG deutet hingegen darauf hin, dass die Pflichten des Verantwortlichen immer greifen sollen, wenn eine automatisierte Entscheidung rechtliche Wirkungen entfalten, ohne dass diese erheblich sein müssten. Es sollte daher klargestellt werden, dass auch diese „rechtlichen Wirkungen“ einen gewissen Schweregrad erreichen müssen. Es ist ferner zu befürchten, dass ein Recht zur „Äusserung“ faktisch zu einer Begründungspflicht führt und damit die Vertragsfreiheit einschränkt. Das ist ein Anliegen des Konsumentenschutzes, das nicht ins Datenschutzrecht gehört. Um übermässige administrative Aufwände zu vermeiden, müssen die Rahmenbedingungen der Information und Anhörung (insbesondere deren Inhalt und der Zeitpunkt) sodann geklärt werden. Wichtig ist dabei, dass die Informationspflicht nach Art. 15 Abs. 1 VE-DSG nur die Angabe

					der Kategorien der Entscheidungen verlangt, die ein Unternehmen automatisiert, und nicht jede einzelne Entscheidung innerhalb dieser Kategorien.
MGB	DSG	16			Eine Datenschutz-Folgenabschätzung muss nach dem VE-DSG erfolgen, wenn eine Datenbearbeitung voraussichtlich zu einem erhöhten Risiko führt. Es ist zunächst klarzustellen, dass ein Risiko für eine Persönlichkeitsverletzung (vgl. Abs. 2 VE-DSG) bestehen muss, nicht für „die Grundrechte“ der betroffenen Personen. Es ist wie schon im geltenden Recht nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG Ausdruck gefunden haben. Gemäss erläuterndem Bericht ist ein erhöhtes Risiko gegeben, wenn die Eigenschaften der geplanten Datenbearbeitung darauf schliessen lassen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann. Das ist enorm breit. Bereits das Versenden einer kritischen E-Mail könnte nach diesen tiefen Anforderungen genügen. Die Voraussetzungen der Datenschutz- Folgenabschätzung müssen daher genauer geregelt werden. In Anlehnung an Art. 35 Abs. 1 DSGVO sollte erst bei einem „hohen“ Risiko eine Pflicht zur Datenschutz- Folgenabschätzung bestehen. Zudem ist es nicht die Aufgabe des Auftragsbearbeiters, die Datenschutz-Folgenabschätzung vorzunehmen. Der Auftragsbearbeiter muss aus der Bestimmung gestrichen werden. Die in Art. 16 Abs. 3 VE-DSG enthaltene Meldepflicht sollte zudem gestrichen oder auf den Fall eingeschränkt werden, dass auch nach Ergreifung angemessener Massnahmen hohe Risiken bleiben. Ohne hohe Restrisiken sollte keine Meldepflicht bestehen. Zudem muss geregelt werden, welche Informationen an den EDÖB weiterzuleiten sind und wie mit diesen insbesondere bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz (BGÖ) umzugehen ist. Datenschutz-Folgenabschätzungen von Unternehmen werden häufig Geschäftsgeheimnisse enthalten, an denen auch die Konkurrenzunternehmen interessiert sind. Die Frist von drei Monaten, die dem EDÖB für die Prüfung der Massnahmen zur Verfügung stehen, ist in der Praxis vollkommen untauglich. Sie muss gestrichen bzw. durch eine angemessene kürzere Frist ersetzt werden.

MGB	DSG	17			Im Gegensatz zur DSGVO und E-SEV 108 findet die Bestimmung im Vorentwurf auf jede Datenschutzverletzung Anwendung. Sie sollte analog zu Art. 4 Nr. 12 DSGVO nur bei Sicherheitsverstössen greifen. Eine Meldung sollte ferner nur erfolgen müssen, wenn eine Vielzahl von Personen betroffen ist. Das ist auch ein Gebot des „nemo tenetur"-Grundsatzes. Der Begriff der Unverzüglichkeit einer Meldung ist weiter zu klären und abzuschwächen. Eine Meldung sollte ohne unnötigen Verzug erfolgen. Eine schnelle Meldung bringt in der Sache nichts, wenn die Hintergründe und Auswirkungen eines Data Breachs noch nicht geklärt sind. Die Pflichten des Auftragsbearbeiters sind auf jene des Verantwortlichen abzustimmen; derzeit besteht hier eine wenn auch nur sprachliche Differenz (keine Information über einen Verlust von Daten).
MGB	DSG	18			Die Formulierung von Art. 18 VE-DSG ist unklar und geht über die in Art. 25 DSGVO enthaltenen Anforderungen hinaus. Art. 18 Abs. 1 VE-DSG gehört zudem systematisch zu 11 VE-DSG, und Art. 18Abs. 2 zu Art. 4 VE-DSG. Art. 18 sollte daher gestrichen und in Art. 4 und 11 VE-DSG integriert werden, wobei nicht über die Anforderungen der DSGVO hinauszugehen ist.
MGB	DSG	19		a	Inhalt und Ausmass der Pflicht zur Dokumentation der Datenbearbeitung gemäss lit. a sollte auf das Führen eines Verzeichnisses aller Datenverarbeitungen beschränkt werden, für die der Verantwortliche zuständig ist. Die Dokumentationspflicht sollte keinesfalls über die in Art. 30 DSGVO enthaltenen Pflichten hinausgehen.
MGB	DSG	19		b	Die Pflicht, die Empfänger von Personendaten über die Berichtigung, Löschung, etc. zu informieren, geht viel zu weit, da ständig Berichtigungen, Löschungen, etc. stattfinden, deren Mitteilung an Empfänger keinerlei Sinn macht (z.B. wenn Daten gelöscht werden, weil sie nicht mehr benötigt werden). Die Informationspflicht darf daher höchstens für die Berichtigung, Löschung und Vernichtung von Daten gelten, nicht jedoch für die Verletzung des Datenschutzes und die Einschränkung der Bearbeitung. Eine Information über Datenschutzverstösse verstösst auch gegen den Grundsatz nemo tenetur. Sie geht sogar weiter als die Pflicht zur Information der betroffenen Person selbst. Die DSGVO sieht auch keine solche Information vor. Die Informationspflicht sollte zudem auf Fälle beschränkt werden, in welchen die betroffene Person dies verlangt und ein schützenswertes Interesse hat. Der Verweis auf einen

					„unverhältnismässigen Aufwand“ genügt nicht. Zudem ist der Auftragsdatenbearbeiter aus dieser Bestimmung zu streichen, da ihm Pflichten auferlegt werden, die er in der Regel nicht erfüllen kann, da er nicht über die erforderlichen Informationen verfügt (beispielsweise über die Richtigkeit der Daten). Sodann sind die Modalitäten der Pflicht unklar. Sie ist auch in dieser Hinsicht auf ein vernünftiges Mass zu beschränken.
MGB	DSG	20			Es fehlt weiterhin an Massnahmen zur Bekämpfung des Missbrauchs des Auskunftsrechts, so namentlich eine zweckentfremdete Nutzung zur Beweismittelausforschung. Es sollten daher bspw. Ausnahmen von der Kostenlosigkeit für Auskunftsersuchen vorgesehen werden (in der DSGVO müssen Auskunftsersuchen ebenfalls nicht zwingend kostenlos sein).
MGB	DSG	20	2	b	Entsprechend der heutigen Regel wäre zu präzisieren, dass die Auskunft nur die Kategorien der bearbeiteten Personendaten beinhalten muss. Dies entspricht auch Art. 15 lit. b DSGVO.
MGB	DSG	20	2	e	Im Rahmen der allgemeinen Auskunftspflicht darf die geforderte Information über automatische Einzelfallentscheidungen nicht eine detaillierte Auflistung aller in der Vergangenheit ausgeführten automatischen Einzelfallentscheidungen verlangen. Vielmehr sollte eine allgemeine Information über automatisierte Einzelfallentscheidungen genügen. Aus diesem Grund ist auch Art. 20 Abs. 3 VE-DSG zu streichen.
MGB	DSG	20	2	g	Art. 20 Abs. 2 lit. g VE-DSG ist an die Streichung von Art. 13 Abs. 4 VE-DSG anzupassen.
MGB	DSG	20	3		Die Pflicht zur Begründung jeglicher Entscheide nach Abs. 3 (nicht nur im Falle von automatisierten Einzelentscheiden) greift massiv in die Freiheit eines Unternehmens ein und geht über das hinaus, was die DSGVO verlangt. Das Auskunftsrecht ist diesbezüglich auf automatisierte Einzelfallentscheide zu beschränken. Geschieht dies nicht, wird auch dieses Auskunftsrecht primär der Ausforschung und Schikane dienen.
MGB	DSG	21			Auch beim Auskunftsrecht, das in Art. 21 Abs. 1 auf Art. 14 VE-DSG verweist, muss die Berufung auf

					überwiegende private Interessen generell – d.h. auch bei Drittweitergaben – zulässig sein. Die wichtigsten Fälle sind zudem exemplarisch aufzuzählen.
MGB	DSG	23			Das Erfordernis der Einwilligung für ein Profiling ist zu streichen. Es besteht weder im bestehenden Recht noch wird es europarechtlich gefordert.
MGB	DSG	24			Der Rechtfertigungsgrund des Abschlusses und der Abwicklung des Vertrags sollte auch die Bearbeitung von Daten weiterer, in den Vertrag involvierten Personen umfassen (z.B. Kontaktperson für Rückfragen).
MGB	DSG	41			Zwar ist nur die private Person, gegen welche sich ein Verfahren richtet, Partei (Art. 44 Abs. 2). Dennoch sieht Art. 41 Abs. 5 VE-DSG die Information über eine Untersuchung auch von anderen Personen vor. Dies verletzt die Geheim- und Privatsphäre des Unternehmens.
MGB	DSG	44			Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben. Die Erfahrungen haben gezeigt, dass der EDÖB vorsorgliche Massnahmen auch ohne vertieftes Abwägen der Folgen verlangt. Eine unabhängige Überprüfungsmöglichkeit ist daher entscheidend. Bis diese stattfindet, muss eine aufschiebende Wirkung bestehen. Es sollte daher dem Gericht überlassen sein zu entscheiden, die aufschiebende Wirkung im Einzelfall zu entziehen (vgl. Art. 55 Abs. 2 VwVG).
MGB	DSG	50 - 55			Die vorgesehenen Strafbestimmungen sind strikt abzulehnen. Sie führen zu einer Kriminalisierung der mit Datenschutz befassten Mitarbeiter. Die gesetzlich gewollten Spielräume bei der Datenbearbeitung werden aus Angst vor persönlicher Bestrafung nicht ausgeschöpft, und es wird unnötige Bürokratie betrieben. Alle Ressourcen werden auf die Einhaltung der formalen, mit Strafe bedrohten flankierenden Massnahmen konzentriert. Das schadet dem Datenschutz. Es wird zudem schwieriger werden, Fachleute für solche Stellen zu gewinnen. Profitieren werden nur die externen Rechtsberater, was die Kosten massiv nach oben treiben wird. Die Sanktionierung Einzelner ist zudem ineffizient, da zwei parallele Verfahren geführt werden müssen (vom EDÖB und von den kantonalen Strafverfolgungsbehörden, die nicht über das erforderliche Know-how verfügen). Ferner ist bei diversen der Antragsdelikte unklar, wer überhaupt antragsberechtigt ist. Zudem fragt sich, ob die Kriminalisierung der Mitarbeiter mit den europarechtlichen Vorgaben vereinbar ist.

					Sowohl die DSGVO als auch die ERK 108 verlangen, dass die Sanktionen nicht nur wirksam und abschreckend sind, sondern auch verhältnismässig. Die Bestrafung einzelner Personen dürfte nicht mehr verhältnismässig sein – ganz sicher nicht bei nur fahrlässigem Verhalten. Zudem fragt sich insbesondere bei Pflichten, deren Erfüllung eine Ermessensentscheidung verlangt, ob sie überhaupt sanktioniert werden dürfen. Beispiele sind Art. 11 (Sicherheit von Personendaten), Art. 16 (Datenschutz-Folgeabschätzung), Art. 18 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen) sowie Art. 19 Abs. 1 (Dokumentation der Datenbearbeitungen). Das strafrechtliche Bestimmtheitsgebot wird hier nicht eingehalten. Auf die Verletzung des Grundsatzes nemo tenetur im Zusammenhang mit den Meldepflichten wurde bereits hingewiesen. Dieses Problem besteht auch im Zusammenhang mit den Kooperationspflichten gegenüber dem EDÖB, soweit es Verhalten betrifft, die für die betroffenen Personen bzw. Unternehmen zu einer Sanktionierung führen können. Auch die Bestrafung fahrlässigen Verhaltens ist nicht sachgerecht und auch europarechtlich nicht erforderlich. Dieses würde die vorstehend beschriebenen unerwünschten Folgen verstärken. Die Begehung des Tatbestandes durch fahrlässiges Verhalten ist daher komplett zu streichen. Eine Sanktionierung sollte nach unserer Ansicht daher primär das Unternehmen betreffen. Wegen der Komplexität vieler datenschutzrechtlicher Sachverhalte (grenzüberschreitende Sachverhalte, zunehmende Arbeitsteilung etc.) ist es kaum je angemessen, einzelne Personen verantwortlich zu machen. Zu denken ist daher an Verwaltungsbussen, die durch den EDÖB zu verhängen wären. Mit dem Wechsel zu verwaltungsrechtlichen, durch den EDÖB verhängten Sanktionen wäre Art. 43 VE-DSG analog Kartellgesetz (KG) auszugestalten, allerdings mit einem wesentlich tieferen Höchstbetrag (z.B. CHF 1 Mio.), denn bei Datenschutzverletzungen wird kaum ein Gewinn erzielt, der wie bei Kartellverstössen eine besonders hohe Busse rechtfertigen könnte. Zudem wirkt bereits das Reputationsrisiko abschreckend. Bei entsprechenden Verfahren und organisatorischen Anforderungen ist sodann den verfassungs- und strafrechtlichen Anforderungen Rechnung zu tragen. Dass die Verfolgungsverjährung auf fünf Jahre ausgedehnt wird, ist ebenfalls nicht nachvollziehbar.
MGB	DSG	52			Für die Verschärfung der heute in Art. 35 DSG geregelten beruflichen Schweigepflicht besteht kein Anlass. Die Verschärfung würde Unternehmen zur Befolgung eines scharfen Berufsgeheimnisses zwingen, für das

					kein Bedarf besteht und das in der Praxis auch nicht gelebt würde. Es ist nicht einzusehen, warum ein Online-Shop denselben Geheimhaltungspflichten wie ein Arzt oder Anwalt unterliegen soll.
MGB	DSG	59			Die Übergangsbestimmungen sind ungenügend. Bedarf für solche gibt es auch bei etlichen anderen der geänderten Regelungen. Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, analog der Regelung der DSGVO.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Philipp Stadler <philipp.stadler@mme.ch>
Gesendet: Montag, 3. April 2017 10:04
An: Amstutz Jonas BJ
Betreff: Stellungnahme Vernehmlassungsverfahren DSG
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_Martin....doc
Signiert von: philipp.stadler@mme.ch

Sehr geehrter Herr Amstutz

Anbei überlasse ich Ihnen die Stellungnahme von Dr. Martin Eckert zu Art. 10 VE-DSG. Gehe ich richtig in der Annahme, dass das Dokument keiner Unterschrift bedarf?

Ich bitte Sie um eine kurze Rückmeldung und danke bereits jetzt herzlich.

Freundliche Grüsse
Philipp Stadler

_____

Philipp Stadler M.A. HSG in Law
Legal Associate

MME Legal | Tax | Compliance
Zurich | Zug
Kreuzstrasse 42 | CH-8032 Zurich | P.O. Box 1412
T +41 44 254 99 66 | F +41 44 254 99 60
philipp.stadler@mme.ch | www.mme.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Dr. Martin Eckert, MME Legal AG

Abkürzung der Firma / Organisation : MME

Adresse : Kreuzstrasse 42, Postfach 1412, 8032 Zürich

Kontaktperson : Dr. Martin Eckert

Telefon : 041 254 99 66

E-Mail : martin.eckert@mme.ch

Datum : 03. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
MME	DSG	10	1 und 2		Sehr geehrte Damen und Herren Im Vernehmlassungsverfahren zur Totalrevision des Schweizer Datenschutzgesetzes reiche ich die nachfolgende Stellungnahme zu Art. 10 VE-DSG ein. Art. 11 Abs. 1 des bestehenden Datenschutzgesetzes (DSG) sieht ein Zertifizierungsverfahren vor. Demgemäss soll es beispielsweise Privatpersonen, die Personendaten im Sinne des DSG verarbeiten, möglich sein, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen zu unterziehen. Gemäss Art. 11 Abs. 2 DSG

					erlässt der Bundesrat dafür und betreffend die Einführung eines Qualitätszeichens Vorschriften. Fakt ist, dass der Bundesrat zwar Vorschriften zu den in Artikel 11 Abs. 1 DSG genannten unabhängigen (privaten) Zertifizierungsstellen erlassen hat (vgl. die Verordnung über die Datenschutzzertifizierungen VDSZ). In Bezug auf die Zertifizierung von Produkten, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten, namentlich Daten über die Benutzerin oder den Benutzer, generiert werden (Art. 5 VDSZ), ist diese Bestimmung bis heute jedoch toter Buchstabe geblieben. Überdies wurde in der Verordnung gänzlich auf die konkrete Regelung bezüglich der Vergabe von entsprechenden Qualitätszeichen bzw. Gütesiegeln verzichtet. Gemäss Art. 5 Abs. 3 VDSZ erlässt der EDÖB Richtlinien darüber, welche datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind. Dazu ist es jedoch nie gekommen. In der digitalen Wirtschaft besteht ein Bedürfnis, Produkte (z.B. Apps) und Dienstleistungen (z.B. Plattformen) zu zertifizieren. Mit sog. Datenschutzgütesiegeln kann in der arbeitsteiligen Wirtschaft Rechtssicherheit geschaffen werden. In der EU sind denn auch private Anbieter sehr erfolgreich etabliert (z.B. www.eprivacy.eu). Gemäss Art. 10a DSG (Art. 7 VE DSG) muss sich der Verantwortliche vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Personen zu gewährleisten. Dieser Vergewisserungspflicht kann der Verantwortliche dann nachkommen, wenn der Auftragsbearbeiter ein Datenschutzgütesiegel nachweisen kann. Die Bestimmung von Art. 11 DSG (Art. 10 VE DSG) wurde mit dem Ziel eingeführt, die Selbstregulierung im Bereich des Datenschutzes zu fördern. Damit soll die Selbstverantwortung der Inhaber der Datensammlungen gestärkt und der Wettbewerb stimuliert werden. Dies trägt zu einer kontinuierlichen Verbesserung von Datenschutz und Datensicherheit bei; bestehende Defizite beim Vollzug der einschlägigen Gesetzgebung können so abgebaut werden. Darüber

					hinaus führt das Konzept der Selbstkontrolle zu einer flexiblen Berücksichtigung der technologischen Entwicklung. Schliesslich soll das Anbringen von Datenschutzgütesiegeln bei den betroffenen Personen das Vertrauen in die korrekte Anwendung der DSG-Richtlinien bzw. die Sicherheit der eigenen und zur Verfügung gestellten Daten steigern (Vgl. Botschaft Revision DSG 2003, 2136). Mit der Vergabe von Datenschutzgütesiegeln akkreditierter Stellen können Unternehmungen das Vertrauen ihrer Kundschaft in ihre angebotenen Produkte bzw. Dienstleistungen steigern. Da sie sich daraus einen Wettbewerbsvorteil versprechen, werden sie animiert, die datenschutzrechtlichen Bestimmungen einzuhalten. So schlägt man gleichsam zwei Fliegen mit einer Klappe. Es gilt jedoch zu beachten, dass die Möglichkeit der Zertifizierung nicht bloss Gross-, sondern auch kleinen und mittleren Unternehmen – die volkswirtschaftlich von enormer Bedeutung sind – offenstehen muss, andernfalls die prophezeiten Resultate gemäss der Botschaft zum DSG (vgl. vorstehend) nicht erreicht werden können. Die Datenschutzgrundverordnung der Europäischen Union (DSGVO), der sich die Schweiz mit der DSG-Revision teilweise annähert, enthält eine zentrale Bestimmung zu diesem Thema. Erwägungsgrund Abs. 100 vor Art. 1 DSGVO besagt (Hervorhebung hinzugefügt): *«Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger* ***Produkte und Dienstleistungen*** *ermöglichen.»* Dies wurde mit Art. 42 DSGVO umgesetzt, der eine Zertifizierung ähnlich derjenigen in Art. 10 VE-DSG vorsieht, wobei gemäss dem Wortlaut der Bestimmung bei den Zertifizierungsverfahren

					den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung zu tragen ist. Gerade Kleinstunternehmen sowie kleine und mittlere Unternehmen profitieren von der Möglichkeit, einzelne Produkte (bspw. Hardwarekomponenten, Software, Online-Kundenplattformen) oder einzelne Dienstleistungen hinsichtlich datenschutzrelevanter Bereiche einer Zertifizierung zu unterziehen. Dies im Gegensatz bspw. zur Zertifizierung von Organisation und Verfahren nach Art. 4 VDVZ (insb. mit Verweis auf die einschlägigen ISO-Normen), bei der es die Zertifizierung von Datenschutzmanagementsystemen geht (Vgl. ausführlich Gabor P. BLECHTA, BSK-DSG, Art. 11 N. 6 ff.). Diese sind für KMUs häufig weder zielführend noch sinnvoll und darüber hinaus schlichtweg zu teuer. Nach alledem wird deutlich, dass gerade KMUs die Möglichkeit zustehen sollte, ihre Produkte und Dienstleistungen möglichst unkompliziert von privaten akkreditierten Zertifizierungsstellen bewerten bzw. sich ein entsprechendes Gütesiegel verleihen zu lassen. Vor diesem Hintergrund ist zu wünschen, dass der Wortlaut von Art. 10 VE-DSG mit einen zusätzlichen Satz analog der Regelung gemäss Artikel 42 DSGVO ergänzt wird: «Den besonderen Bedürfnissen von Kleinstunternehmen und kleinen und mittleren Unternehmen wird Rechnung getragen.» In diesem Sinne sollte auch der Auftrag an den Bundesrat bzw. indirekt an den EDÖB unmissverständlich dahingehend formuliert werden, dass die obigen Ziele (Zertifizierung von Produkten und Dienstleistungen) auch faktisch bzw. tatsächlich erreicht werden können. Es wäre schade, wenn die Bestimmung von Art. 10 VE-DSG (in Bezug auf die Produktezertifizierung) wie Art. 11 DSG toter Buchstabe bliebe. Freundliche Grüsse Dr. Martin Eckert
Fehler! Verweisquelle konnte nicht gefunden werden.					

Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

MS Direct AG
Hauptsitz
Fürstenlandstrasse 35
CH-9001 St. Gallen

Telefon +41 71 274 66 66
contact@ms-direct.ch
www.ms-direct.ch

UID CHE-101.130.427

mit Standorten in Meilen,
Muttenz, Wittenbach,
Adligenswil, Lauterach (AT)

MS Direct AG · Fürstenlandstrasse 35 · CH-9001 St. Gallen

Per E-Mail an jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und Polizeidepartement
EJPD
Bundesamt für Justiz
Bundesrain 20
CH 3003 Bern

St. Gallen, 4. April 2017

Stellungnahme der MS Direct AG zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die MS Direct AG tritt als Gesamtanbieterin von massgeschneiderten Lösungen und ganzheitlichen Services für Kundenbeziehungsmanagement und E-Commerce im Markt auf und bietet einen Full Service Provider für Unternehmen an, die sich auf ihre Kernkompetenzen konzentrieren möchten. Wir sind ein innovatives Schweizer Familienunternehmen mit rund 900 Mitarbeitenden in St. Gallen (Hauptsitz), Meilen, Muttenz, Wittenbach, Adligenswil und Lauterach (Österreich). Unsere Leistungsbereiche sind CRM Solutions, Customer Services, Direct Marketing, E – Commerce Solutions und Logistic Services. Durch diese breitgefächterten Tätigkeiten sind wir von der Revision des Datenschutzgesetzes stark betroffen.

Wir begrüssen die angestrebte Modernisierung des Datenschutzrechts und die beabsichtigte Annäherung an die künftige Rechtslage in der EU. Wir sehen auch die gesamtwirtschaftliche Bedeutung und Wichtigkeit der Möglichkeiten der Datenbearbeitungen zu Werbezwecken und des Vertrauens in diese Datenbearbeitungen. Wir vertreten aber konsequent die Haltung, dass es hierfür keinesfalls erforderlich ist, über die Vorgaben der E-SEV 108 und der EU-DSGVO hinauszugehen.

Deshalb lehnen wir grundsätzlich jede Änderungen gegenüber der geltenden Rechtslage ab, die zur Einhaltung der Vorgaben der Europarats-Konvention (E-SEV 108) oder mit Blick auf die Angemessenheits-Beurteilung des Schweizer Datenschutzrechts durch die EU nicht zwingend geboten sind

(sog. „Swiss Finish"). Insbesondere kostenerhöhende Vorschriften, welche dazu führen, dass die administrativen Kosten und Aufwände und damit die Kosten der betreffenden Werbeaktivitäten zunehmen, sind für uns nur dann annehmbar, wenn zwingende Vorgaben der Datenschutzkonvention des Europarates dies fordern.

Das Gesagte gilt insbesondere für den „Swiss Finish" bei der vorgeschlagenen Regelung des „Profiling" und der Sanktionierung von Verstössen, welche wir entschieden ablehnen.

In der aktuellen Fassung müssen wir deshalb den Vorentwurf des neuen DSG ablehnen. Das angedachte Sanktionssystem, mit dem eine Kriminalisierung von natürlichen Personen in einem erheblichen Umfang in datenbearbeitenden Unternehmen erfolgt, kann so nicht angenommen werden. Die direkte Bestrafung der wirtschaftlich verantwortlichen Unternehmen ist der einzig vertretbare Weg.

Weiter behindert dieses Sanktionssystem die Innovationskraft und das Innovationspotential der Digitalen Wirtschaft in der Schweiz und insbesondere der Schweizer KMU: Die Risikobeurteilung bei Innovationen in der „Data Economy" müsste künftig immer im Licht einer möglichen strafrechtlichen Verfolgung der Mitarbeiter, welche in diesen Unternehmen tätig sind, vorgenommen werden. Eine aus unserer Sicht unhaltbare Situation, welche wirtschaftshemmend ist. Ein solches Sanktionssystem stellt die zentrale Anerkennung der Angemessenheit des Schweizer Datenschutzniveaus in keiner Weise sicher. Bei allen Firmen, welche grenzüberschreitend tätig sind, können Sanktionen gegenüber Datenbearbeitern aus dem Ausland faktisch nicht durchgesetzt werden und in den meisten Fällen wären sie auch rechtlich nicht vollstreckbar.

Wir legen Ihnen unsere detaillierte Stellungnahme zu den einzelnen Normen des Vorentwurfs bei. Wir danken Ihnen, dass Sie uns Gelegenheit geben, zu dieser für unser Unternehmen wichtigen Gesetzesrevision Stellung zu nehmen.

Freundliche Grüsse

Myrio Kluser
Head CRM & Datamanagement

CRM Solutions
Customer Services
Direct Marketing Services
E-Commerce Solutions
Logistic Services

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : MS Direct AG

Abkürzung der Firma / Organisation : MSD

Adresse : Fürstenlandstrasse 35, 9001 St. Gallen

Kontaktperson : Myrio Kluser

Telefon : 044 925 36 36

E-Mail : myrio.kluser@ms-direct.ch

Datum : 04.04.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
MSD	Grundsätzlich unterstützen wir die Revision des DSG und die damit verbundene Annäherung an die EU Normen. Im Weiteren sehen wir die Notwendigkeit die Voraussetzung für den grenzüberschreitenden Datenverkehr und die damit entstehende Rechtssicherheit zu schaffen. Wir erachten es aber als nicht notwendig, ja sogar wettbewerbsbenachteiligend, wenn die Schweizer Regelungen, resp. Anforderungen weiter gehen als diejenigen der EU. Hier sehen wir eine klare Benachteiligung der MS Direct gegenüber ihren Wettbewerbern in EU Raum.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
MSD	DSG	1			Im Weiteren soll die Voraussetzung für den grenzüberschreitenden Personendatenverkehr geschaffen werden.
MSD	DSG	2	1		-
MSD	DSG	3		a	Die Beibehaltung der Definition von Personendaten ist zu begrüssen. Ebenfalls der Verzicht auf die juristischen Personen. Eine Präzisierung der Bestimmbarkeit einer Person wäre notwenig und zu begrüssen.
MSD	DSG	3		c. 4.	Der Begriff der biometrischen Daten ist zu präzisieren.
MSD	DSG	3		f	Betreffend Profilling sollte die CH Regelung nicht weitergehen, als diejenige der EU.
MSD	DSG	4			-
MSD	DSG	4	3		-
MSD	DSG	4	5		Bisherige Definition beibehalten (Art. 5 Abs. 1 DSG).
MSD	DSG	4	6		Präzisierungen der Erfordernisse wären wünschenswert. Im Weiteren soll die Regelung nicht strenger sein, als diejenigen der EU.

MSD	DSG	5	3-6		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	6	1	B	Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	6	2		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	7			-
MSD	DSG	8			Präzisierung, wer zu den interessierten Kreisen gehört.
MSD	DSG	8	1		Kompetenzen des EDÖB sind zu reduzieren, da sonst Entschiede im Alleingang gefällt werden können.
MSD	DSG	8	2		-
MSD	DSG	12			Erben sollen nicht mehr Rechte erhalten als die Verstorbenen zu Lebzeiten hatten.
MSD	DSG	13			Auf die Informationspflicht bei der Beschaffung von Daten bei Dritten ist zu verzichten, da dies für Unternehmen kaum praktikabel ist.
MSD	DSG	13	2		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	13	4		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	13	5		Auf die Informationspflicht bei der Beschaffung von Daten bei Dritten ist zu verzichten, da dies für Unternehmen kaum praktikabel ist.
MSD	DSG	14			Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	15			Regelung soll nicht strenger sein, als diejenige der EU.

MSD	DSG	16			Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	17	1		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	17	2		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	18			-
MSD	DSG	19			Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	19		A	Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	19		B	Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	20	1		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	20	3		Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	23			Regelung soll nicht strenger sein, als diejenige der EU.
MSD	DSG	23	3		-
MSD	DSG	24	2		Der MSD fordert, dass entsprechend der EU-DSGVO (Erw.-Gr. 47) zumindest in der Botschaft darauf hinzuweisen ist, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
MSD	DSG	24	2	a.	-
MSD	DSG	24	2	C3	Streichung des Passus
MSD	DSG	25			-

MSD	DSG	37-49			-
MSD	DSG	44	3		-
MSD	DSG	50 ff.			Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt.
MSD	DSG	52			-
MSD	DSG	55			-

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
MSD	3 lit. A	-
MSD	3 lit. f	Der Begriff des Profiling ist zu präzisieren
MSD	4 Abs. 6	-
MSD	8	-
MSD	13	-
MSD	15	-

MSD	18	-
MSD	23 Abs. 3	-
MSD	24 Abs. 2	-
MSD	50 ff	Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt.
MSD	Seite 64	-
MSD	Seite 88	-

Amstutz Jonas BJ

Von: Roberto Balmer <roberto.balmer@outlook.com>
Gesendet: Dienstag, 4. April 2017 23:48
An: Amstutz Jonas BJ
Cc: robi@nüglarus.ch
Betreff: Stellungnahme NüGlarus zur Revision DSG
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de nüglarus.doc

Sehr geehrter Herr Amstutz

Im Anhang finden Sie die Anpassungsvorschläge zu Art 50 DSG (Einführung Widerspruchsverfahren analog Kartellgesetz) und Art 54 DSG (Ausnahmen für Startups im Gesundheitsbereich) des Vereins NüGlarus. Die Vorschläge sind EU-kompatibel, da sowohl Verfahrensanpassungen wie Ausnahmen keine materiellen Anpassungen am Gesetz bedingen.

Als lokale und nicht profit-orientierte digitale Plattform, welche den ganzen Kanton, also Wirtschaft, Gesellschaft und Verwaltung, bei seinem Innovationsprozess unterstützt, ist es uns ein grosses Anliegen, dass neue innovative Geschäftsmodelle und Startups durch das neue DSG nicht ver- oder behindert werden. Mehr Informationen zu unserer Initiative finden Sie auf http://www.nüglarus.ch.

Bei Fragen stehe ich Ihnen gern zur Verfügung.

Mit freundlichen Grüssen

Roberto Balmer
Präsident
0798828351

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verein NüGlarus

Abkürzung der Firma / Organisation : NüGlarus

Adresse : c/o Handelskammer, Postgasse 27, 8750 Glarus

Kontaktperson : Roberto Balmer

Telefon : 0798828351

E-Mail : robi@nüglarus.ch

Datum : 4.4.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht	DSG	50-54			Das neue Datenschutzgesetz weitet die Regulierungkosten für Unternehmen im Datenschutzbereich sehr stark aus. Für Startups stellen diese teils prohibitive Eintrittshürden in digitale neue Geschäftsfelder dar. Um sicherzustellen, dass die Schweiz nicht wie der Rest Europas hinter die Innovationskraft der USA

gefunden werden. NüGlarus					zurückfällt, sind folgende Anpassungen vorzunehmen, welche die grundsätzliche Angemessenheit des Datenschutzgesetzes aus Sicht der EU nicht in Frage stellen:
Fehler! Verweisquelle konnte nicht gefunden werden. NüGlarus	DSG	50			1. Die Regulierungskosten sind nur soweit absolut notwendig auf die innovierenden Unternehmen und im speziellen Startups zu überwälzen. Der Bund muss Unternehmen bei der Umsetzung dieses Gesetzes daher unterstützen. Dazu ist analog dem Schweizer Kartellgesetz (Art. 49a Abs. 3 KG) ein Widerspruchsverfahren einzuführen. Es ist also folgender Artikel im DSG aufzunehmen: ***Art. 50a*** ***Eine Sanktion entfällt, wenn Unternehmen ihre Unternehmensprozesse melden, bevor diese Wirkung entfalten. Wird dem Unternehmen innert drei Monaten nach der Meldung die Verletzung von Datenschutzbestimmungen mitgeteilt und hält es danach an seinen Prozessen fest, entfällt die Belastung nicht.*** Bei der Umsetzung dieses Gesetzes soll der Bund zur Kostenreduktion Funktionen auch auslagern können.
Fehler! Verweisquelle konnte nicht gefunden werden. NüGlarus	DSG	54			2. Selbst mit einem Widerspruchsverfahren werden sich die Regulierungskosten von Startups im Datenbereich derart erhöhen, dass viele Businessmodelle nicht mehr möglich sind. Hier muss ein Gleichgewicht geschaffen werden. Wenn zum Beispiel ein kleines Krebsforschungs-Startup seine Forschung einstellen muss, da es sich keine Datenschutzexperten leisten kann und dadurch Forschungsresultate verhindert werden, die Leben retten könnten, dürfte dies kaum im öffentlichen Interesse sein. Bei grösseren Unternehmen, welche schon länger auf dem Markt sind, ist diese Innovations-Behinderung weniger ausgeprägt. Es ist daher zumindest folgende begrenzte Ausnahme zu schaffen: **Artikel 54a** **Dieses Gesetz findet keine Anwendung auf Unternehmen, welche:** **1. vor weniger als fünf Jahren gegründet wurden, und**

					2. einen Umsatz von unter fünf Milionen Franken pro Jahr erwirtschaften, und **3. vollständig oder teilweise Dienstleistungen für das Gesundheitswesen erbringen, und** **4. ihren Sitz in einem strukturell schwachen Kanton mit Durchschnittseinkommen, welche mindestens 10 Prozent unter dem Schweizer Durschnitt liegen, haben**
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht	

gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden	

werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Bretschger Roman <roman.bretschger@nzz.ch>
Gesendet: Dienstag, 4. April 2017 15:23
An: Amstutz Jonas BJ
Betreff: Totalrevision des Datenschutzgesetzes - Stellungnahme NZZ-Mediengruppe
Anlagen: Totalrevision-des-Datenschutzgesetzes_Stellungnahme_NZZ.doc

Sehr geehrter Herr Amstutz

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Vorentwurf des Bundesgesetzes über den Datenschutz. Gerne senden wir Ihnen hiermit fristgerecht unsere Stellungnahme im Anhang.

Für Rückfragen stehen wir Ihnen selbstverständlich jederzeit sehr gerne zur Verfügung.

Mit freundlichen Grüssen
Roman Bretschger

NZZ-MEDIENGRUPPE

Dr. Roman Bretschger, LL.M.
Rechtsanwalt / Generalsekretariat

NZZ Management AG
Falkenstrasse 11 · CH-8021 Zürich
Zentrale +41 44 258 11 11 · Direkt +41 44 258 14 54
roman.bretschger@nzz.ch · www.nzzmediengruppe.ch

Stellungnahme von

Name / Firma / Organisation : NZZ-Mediengruppe

Abkürzung der Firma / Organisation : NZZ

Adresse : Falkenstrasse 11, 8008 Zürich

Kontaktperson : Dr. Roman Bretschger, Rechtsanwalt

Telefon : 044 258 14 54

E-Mail : roman.bretschger@nzz.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
	Die Kernanliegen der Datenschutzrevision sind eine Stärkung des Datenschutzes durch Schaffung von mehr Transparenz und Kontrollmöglichkeiten bei gleichzeitiger Erhaltung der Möglichkeit des grenzüberschreitenden Datenaustausches mit der EU, wobei gemäss Ausführungen von Frau Bundesrätin Simonetta Sommaruga im Begleitschreiben zur Vernehmlassung die staatlichen Eingriffe auf ein Minimum beschränkt werden sollen. Diese angestrebten Ziele wiederspiegeln sich im Vorentwurf des Bundesgesetzes über den Datenschutz (VE-DSG) eindeutig nicht. Im Gegenteil: es ist eine umfassende Regulierung sämtlicher innerbetrieblichen Vorgänge, die mit der Bearbeitung von Personendaten zusammenhängen, vorgesehen, komplementiert mit weitreichenden Notifikationspflichten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie einem umfangreichen Sanktionskatalog von Strafbestimmungen, falls einer der beiden ersten Punkte auf irgendeine Art und Weise nicht oder nicht richtig umgesetzt worden ist. Aus Sicht eines Medienunternehmens fällt zudem auf, dass der VE-DSG zudem viele Bestimmungen enthält, welche die journalistische Arbeit erschweren bis verunmöglichen werden, müssten diese umfassend eingehalten werden. Zweifellos war es nicht die Absicht, Journalisten Steine in den Weg zu legen, aber manche der Bestimmungen sind in ihren Konsequenzen nicht wirklich durchdacht und werden genau diesen Effekt haben. Damit droht der Datenschutz nach Vorgabe des VE-DSG die Funktion der Medien für eine freie Demokratie nachhaltig zu untergraben, was wohl niemand will. Der NZZ-Mediengruppe ist es daher daran gelegen, einige der gravierendsten Mängel der VE-DSG im Rahmen der «Allgemeinen Bemerkungen» aufzugreifen. Wir verzichten hingegen darauf, zu sämtlichen Artikeln im Detail Stellung zu nehmen; dies verbunden mit der Hoffnung und der Bitte, zumindest diese ganz zentralen Punkte im Rahmen des weiteren Gesetzgebungsprozesses zu berücksichtigen. Für eine Besprechung sämtlicher Artikel im Detail verweisen wir im Übrigen auf die Eingabe des Verbandes Schweizer Medien (VMS).
	Kein «Swiss Finish» Die europäischen Entwicklungen im Datenschutzrecht machen gewisse Anpassungen erforderlich. Der grenzüberschreitende Austausch von Personendaten muss möglich bleiben, weshalb ein inhaltlich gegenüber der EU gleichwertiger Datenschutz zu erhalten ist. Doch der VE-DSG übernimmt die Regulierungen der Europäischen Datenschutzgrundverordnung (DSGVO) nicht nur weitgehend, sondern verschärft diese gar noch in verschiedenen Belangen, die für die Schweizer Unternehmen sehr nachteilig wären. Für einen solchen "Swiss Finish" gibt es keinerlei Anlass und keinen Grund. **Sämtliche Verschärfungen gegenüber den Regelungen der DSGVO sind daher aus dem VE-DSG zu entfernen.**

	<u>Kein Sanktionsregime mit neuen Straftatbeständen (Art. 50 ff. VE-DSG)</u> Besonders standortschädlich und abzulehnen ist das vorgeschlagene Sanktionswesen mit neuen Straftatbeständen. Der Verzicht auf drakonische Sanktionen im Stile der DSGVO (Bussen bis zum höheren Betrag von EUR 20 Mio. oder 4% des letzten weltweit erzielten Jahresumsatzes) ist zwar zu begrüssen. Der VE-DSG setzt hingegen darauf, die Verletzung von administrativen Nebenpflichten neu als Straftatbestände auszugestalten. Ins Visier geraten damit die natürlichen Personen in der Schweiz, welche für die Datenbearbeitung in Unternehmen verantwortlich sind. Nur wenn sich diese nicht identifizieren lassen, soll subsidiär das Unternehmen mit maximal CHF 100'000.00 gebüsst werden. Diese nicht sachgerechte Kriminalisierung jedes einzelnen Mitarbeiters eines Unternehmens ist abzulehnen. Schweizer Unternehmen – besonders KMU – müssten ihre Mitarbeiter mit grossem Compliance-Aufwand schützen und würden sich im Zweifel für eine konservativere Methode der Datenbearbeitung entscheiden. Sie gefährdet den allgemeinen und sich als gewinnbringend erweisenden risikobasierten Ansatz dahingehend, als dass der gesetzlich vorgegebene und wirtschaftlich betrachtet äusserst sinnvolle Anwendungsspielraum aus Angst vor Sanktionen nicht mehr ausgeschöpft wird. Stattdessen werden die Unternehmen und ihre Mitarbeiter stets den bürokratisch aufwändigen aber rechtlich absolut sicheren Weg wählen. Der Ausbau der Bürokratie zwecks Selbstschutz kann nicht Sinn der Sache sein, doch wird der VE-DSG genau dies bewirken. Diese neuen Straftatbestände sind daher entschieden abzulehnen. Die NZZ-Mediengruppe vertritt daher dezidiert die Auffassung, dass **der Katalog der Strafbestimmungen auf den heute geltenden Katalog der Strafbestimmungen reduziert werden muss**. Falls dieser Katalog dennoch ausgebaut werden soll, so darf eine Verletzung von Datenschutzbestimmungen nur in der (verhältnismässigen) Sanktionierung des datenbearbeitenden Unternehmens resultieren. **Die persönliche Strafbarkeit von Mitarbeitern und die fahrlässige Tatvariante ist ersatzlos zu streichen.**
	<u>Verzicht auf bzw. Einschränkung des «Profiling» (Art. 3 lit. f. und Art. 23 lit. d VE-DSG).</u> Neu wird der Begriff des «Profiling» eingeführt. Im Gegensatz zum Begriff des Profilings in der DSGVO ist die Definition in der VE-DSG extrem breit. Ein Profiling nach VE-DSG liegt nicht nur bei einer automatisierten, sondern bei jeder Auswertung von Daten vor. Dies bedeutet unter anderem, dass fast jede journalistische Recherche als Profiling zu qualifizieren ist. Dies ist deshalb höchst problematisch, weil gemäss VE-DSG ohne Begründung jedes Profiling per Generalverdacht eine Persönlichkeitsverletzung darstellen soll, obwohl der Begriff des Profiling derart breit definiert ist, dass er auch unzählige alltägliche und völlig harmlose Handlungen erfasst. Diese Regel hat wiederum zur Folge, dass Profiling damit nur mit einem Rechtfertigungsgrund erfolgen darf, also beispielsweise einer vorgängig eingeholten ausdrücklichen Einwilligung oder einem überwiegenden Interesse. Mit anderen Worten muss zum Beispiel ein Journalist vor jeder Recherche, selbst wenn es sich hierbei um eine manuelle Recherche für einen Artikel handelt, zuerst bezüglich der diversen davon betroffenen Personen Einwilligungen einholen oder entsprechende überwiegende Interessen dokumentieren. Aber auch datengetriebene Geschäftsmodelle wie beispielsweise dasjenige der Moneyhouse AG würden dadurch faktisch verunmöglicht. Diese Regelung ist völlig unverhältnismässig. In

	Anbetracht all dieser Gründe sollte **der Begriff des Profilings komplett gestrichen werden**; es braucht ihn nicht, eine Regel über automatisierte Einzelentscheide reicht aus. Sofern am Begriff des Profilings festgehalten wird, sollte er zumindest **auf automatisierte Datenbearbeitungen beschränkt werden.**
	<u>Falsches bzw. unklares Konzept der «Einwilligung» (Art. 4 Abs. 6 VE-DSG)</u> Gemäss dem Wortlaut des VE-DSG muss eine Einwilligung «eindeutig» erfolgen. Was das bedeutet, geht weder aus dem Gesetzeswortlaut noch aus dem Erläuterungsbericht hervor. Auch in Bezug auf die «Ausdrücklichkeit» der Einwilligung, die es im Zusammenhang mit besonders schützenswerten Personendaten und Profiling braucht, schafft der Erläuterungsbericht mehr Verwirrung als Klarheit. Hierfür gibt es keinen vernünftigen Grund. Die Einwilligung ist eine Willenserklärung wie jede andere auch. **Zumindest auf das Konzept der «Eindeutigkeit» sollte daher verzichtet werden**. Zwar begrüsst es die NZZ-Mediengruppe, dass im VE-DSG von den in der DSGVO vorgesehenen Einschränkungen im Zusammenhang mit Einwilligungen im Datenschutz klar Abstand genommen wird und demnach weder ein Koppelungsverbot eingeführt wird noch, dass eine Einwilligung erst dann unmissverständlich sein soll, wenn diese durch eine eindeutige bestätigende Handlung vorgenommen wird. Dafür bleibt im Schweizer Recht denn auch kein Platz. Die Einwilligung ist eine Willenserklärung wie jede andere auch und bemisst sich nach den Bestimmungen des allgemeinen Obligationenrechts, was insbesondere bedeutet, dass eine ausdrückliche Einwilligung vorliegt, wenn der Sinngehalt der Willenserklärung ausdrücklich aus dieser selbst hervorgeht, ohne dass notwendigerweise zur Deutung weitere Umstände herangezogen werden müssen. Angesichts der wichtigen praktischen Bedeutung der Möglichkeit einer stillschweigenden Übernahme von Allgemeinen Geschäftsbedingungen (AGB) und aufgrund der bestehenden Unsicherheit im Zusammenhang mit Datenbearbeitungen soll dies zumindest in der Botschaft klar zum Ausdruck kommen. Schliesslich ist die NZZ-Mediengruppe der Meinung, dass sich **für das Profiling – sollte der Begriff beibehalten werden – keine ausdrückliche Einwilligung rechtfertigt**, da es sich hierbei in Wirklichkeit um alltägliche Datenbearbeitungen handelt und nicht, wie mit dieser Bestimmung suggeriert wird, um besonders bedrohliche oder für die Persönlichkeit der betroffenen Personen heikle Projekte. Solche kann es vereinzelt geben, aber das rechtfertigt nicht die Sonderbehandlung.
	<u>Kein unnötiger Compliance-Aufwand (Art. 13, 16 und 17 VE-DSG)</u> Die VE-DSG enthält schliesslich diverse Regelungen, welche bloss einen internen administrativen Mehraufwand bewirken, Compliance-Kosten erhöhen, aber keinerlei Mehrwert im Hinblick auf den Persönlichkeitsschutz der betroffenen Personen – dies das Kernanliegen der Revision – bringen und zudem den EDÖB mit einer Flut von Notifikationen, Informationen und Anfragen überlasten. Als erstes Beispiel ist die **Informationspflicht** zu nennen. Die Ausweitung der Informationspflichten auf alle Personendaten wird zu einem

	enormen Mehraufwand für Schweizer Unternehmen jeder Grösse führen, falls die denn im vorgesehenen Umfang überhaupt umgesetzt werden können. Einen sachlichen Grund für diese Ausweitung gibt es nicht. Bereits nach geltendem Recht gilt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angezeigt wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Diese Lösung berücksichtigt im Rahmen eines Bearbeitungsgrundsatzes das Risiko der jeweiligen Datenerhebung und mögliche Rechtfertigungsgründe. Dies ist ausreichend, um gegenüber der betroffenen Person Transparenz in Bezug auf die Datenerhebung und den mit der Bearbeitung verbundenen Zweck zu wahren. Eine darüberhinausgehende Regulierung und die damit einhergehende Formalisierung von Informationen wird in einer Flut von Schildern, Nutzungsbedingungen, Privacy Notices, Policies u.ä. resultieren, welche letztlich bekanntermassen von niemandem gelesen werden. Damit wird das exakte Gegenteil von Transparenz bewirkt. Es wäre einer erhöhten Transparenz und damit einem realistischen Effekt viel dienlicher, den Fokus auf das Wesentliche (also auf wenige dafür entscheidende Informationen) zu legen als die Informationsverpflichtungen immer weiter auszubauen, womit die Unübersichtlichkeit erhöht und Transparenz verhindert wird. Insofern zielt die Revision genau in die falsche Richtung. **Auf die Ausweitung der Informationspflichten ist daher zu verzichten, diese sollten sich (der Transparenz halber) auf das Wesentliche beschränken.** Als zweites Beispiel kann die Durchführung einer **Datenschutz-Folgeabschätzung** bei einem "voraussichtlich erhöhten Risiko" genannt werden. Dies ist zum einen ein unklarer und damit für die betroffenen Unternehmen unbrauchbarer Begriff, weil daraus nicht hervorgeht, gegenüber was eine Erhöhung des Risikos vorliegen muss. Zum anderen stellt jede einzelne Datenbearbeitung – gerade in Unternehmen – immer ein erhöhtes Risiko dar, weshalb diese Voraussetzung per se untauglich ist. Müsste man für jede Bearbeitung (im Falle von Medien: Dem Verfassen jedes einzelnen Beitrags über eine natürliche Person) ein formalisiertes Beurteilungsverfahren durchführen, wäre dies uferlos. **In keinem Fall darf die Schwelle nach Schweizer DSG daher unter diejenige der DSGVO fallen**; darin wird immerhin von einem "hohen" Risiko gesprochen. **Die pauschale Meldepflicht der Datenschutz-Folgeabschätzung an den EDÖB muss zudem gestrichen werden.** Als drittes Beispiel können schliesslich die **Meldepflichten** an den EDÖB bei unbefugter Datenbearbeitung oder Datenverlust genannt werden. Die Umsetzung dieser Verpflichtung hätte zur Folge, dass jede unbefugte Datenbearbeitung, namentlich jede Datenbearbeitung die einem Grundsatz gemäss Art. 4 ff. VE-DSG widerspricht (also beispielsweise auch eine unverhältnismässige Datenverarbeitung), dem EDÖB gemeldet werden muss. Dies ist nicht nur völlig unverhältnismässig. Ausserdem muss die parallele Strafbewehrung des Verstosses an sich und der Meldepflicht ebendieses Verstosses rechtsstaatlich als höchst bedenklich eingestuft werden (*nemo tenetur*) und wird wohl letztlich zu einer Unternehmensstruktur mit vollständiger Überwachung der Mitarbeiter und Pflicht zum gegenseitigen Verrat führen. **Es würde völlig genügen, wenn lediglich jene *Data Breaches* gemeldet werden müssten, bei denen so viele Personen so massiv betroffen sind, dass es sinnvoll ist, dass eine Behörde überprüft, ob die nötigen Schutzvorkehrungen getroffen worden sind** (die sich schon aus dem geltenden DSG ergeben). So wie sich die Regelung heute präsentiert, müsste jede Zeitungsmeldung, die einen Fehler mit Bezug auf eine natürliche Person enthält, dem EDÖB unverzüglich gemeldet werden.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)					
Name/Firma	**Gesetz**	**Art.**	**Abs.**	**Bst.**	**Bemerkung/Anregung**
					Wie eingangs erwähnt wird für die umfassende Kommentierung der einzelnen Artikel auf die Eingabe des Verbandes Schweizer Medien (VSM) verwiesen.

Amstutz Jonas BJ

Von: Parlamentarische Gruppe Digitale Nachhaltigkeit <info@digitale-nachhaltigkeit.ch>
Gesendet: Dienstag, 4. April 2017 19:12
An: Amstutz Jonas BJ
Betreff: Parldigi Vernehmlassungsantwort DSG-Revision
Anlagen: Parldigi Vernehmlassungsantwort DSG-Revision.pdf; Parldigi Vernehmlassungsantwort DSG-Revision.odt

Sehr geehrter Herr Amstutz

Anbei schicken wir Ihnen unsere Vernehmlassungsantwort zur DSG-Revision.

Freundliche Grüsse,

Matthias Stürmer

Parlamentarische Gruppe Digitale Nachhaltigkeit
Dr. Matthias Stürmer, Geschäftsleiter
Engehaldenstrasse 8
3012 Bern

Telefon: +41 31 631 38 09
Mobile: +41 76 368 81 65
info@digitale-nachhaltigkeit.ch
http://www.digitale-nachhaltigkeit.ch

Parldigi

Parlamentarische Gruppe Digitale Nachhaltigkeit
c/o CH Open
Engehaldenstrasse 8
3012 Bern

Bern, 4. April 2017

Vernehmlassungsantwort der Parlamentarischen Gruppe Digitale Nachhaltigkeit zum Entwurf des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Die Parlamentarische Gruppe Digitale Nachhaltigkeit Parldigi nimmt gerne die Gelegenheit wahr, sich im Rahmen der Vernehmlassung zur Revision des Datenschutzgesetzes (DSG) zu äussern.

Parldigi begrüsst die Totalrevision des Datenschutzgesetzes und unterstützt die Anpassung des Schweizer DSG in Richtung EU-Standards, wodurch die Schweiz weiterhin als Drittstaat mit angemessenem Datenschutzniveau anerkannt wird. Ein griffiges Datenschutzgesetz wirkt sich positiv auf den Wirtschaftsstandort Schweiz aus, da ein starker Datenschutz sowohl für die Schweizer Bevölkerung als auch für ausländische Kundinnen und Kunden attraktiv ist.

Folgende Punkte sind bezüglich digitaler Nachhaltigkeit relevant:

1. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Die Regelung zu „Privacy by Design" und „Privacy by Default" von Art. 18 VE-DSG wird unterstützt.

Es ist sinnvoll, die Pflicht zum Datenschutz durch Technik sowie durch datenschutzfreundliche Voreinstellungen einzuführen. Durch das frühzeitige Treffen von Massnahmen gegen Verletzungen der Persönlichkeit oder der Grundrechte in der Planungsphase einer Datenbearbeitung kann das Risiko von Datenmissbrauch spürbar eingeschränkt werden.
Durch datenschutzfreundliche Technik kann der Bedarf nach rechtlichen Regeln reduziert werden, indem die Möglichkeit eines Verstosses gegen Datenschutzvorschriften erheblich erschwert oder gar verunmöglicht wird. Ebenfalls die Einführung der Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen, durch welche lediglich die für den jeweiligen Verwendungszweck minimal erforderlichen Daten bearbeitet werden, ist zu begrüssen.
Werden „Privacy by Design" und „Privacy by Default" nicht im DSG aufgenommen, besteht die Gefahr, dass das schweizerische Datenschutzgesetz im Vergleich zur EU-Verordnung nicht als gleichwertig anerkannt wird.

2. Recht auf Datenportabilität

Das Recht auf Datenportabilität soll nach dem Vorbild von Art. 20 DSGVO in das DSG übernommen werden.

Das Recht auf Datenportabilität erlaubt den Betroffenen die personenbezogenen Daten, die sie einem Bearbeiter zur Verfügung gestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und an einen anderen Datenbearbeiter zu übermitteln. So können Personen ihre persönlichen Daten flexibel bei verschiedenen Bearbeitern nutzen und reduzieren dadurch die Abhängigkeit von einzelnen Firmen.

Da es die direkte Übermittlung von personenbezogenen Daten von einem Datenbearbeiter zum anderen ermöglicht, ist das Recht auf Datenportabilität auch ein wichtiges Instrument, das den freien Datenfluss in der EU unterstützt und den Wettbewerb zwischen den Bearbeitern fördert. Der Umstieg zwischen verschiedenen Dienstleistern wird erleichtert und damit die Entwicklung neuer Dienstleistungen im Rahmen der digitalen Binnenmarktstrategie unterstützt.

3. Stärkung der Stellung und Ausbau der Befugnisse und Aufgaben des Beauftragten

Parldigi begrüsst die Stärkung der Rolle des EDÖB durch Art. 37 ff. VE-DSG.

Es ist angemessen, dass der Datenschutzbeauftragte – wie seine Kolleginnen und Kollegen in den anderen europäischen Ländern – nach Abschluss einer Untersuchung, die von Amtes wegen oder auf Anzeige hin eingeleitet wurde, Verfügungen erlassen kann, die für die Verantwortlichen und die Auftragsbearbeiter verbindlich sind.

4. Angleichung der finanziellen Strafbestimmungen an EU-Verordnung

Parldigi begrüsst die Erhöhung der Bussen von maximalen CHF 10'000 auf CHF 500'000, würde jedoch eine Angleichung der Busshöhe an die EU-Verordnung begrüssen.

Art. 83 Abs. 4-6 DSGVO erhöht den Bussgeldrahmen für Datenschutzverstösse drastisch und vereinheitlicht ihn europaweit. In Art. 83 Abs. 4 DSGVO ist ein Bussgeldrahmen von bis zu € 10 Mio. vorgesehen; gemäss Art. 83 Abs. 5 und 6 sogar bis zu € 20 Mio. oder 4% des weltweiten Jahresumsatzes. Um im Vergleich zur Regelung in der EU-DSGVO nicht wieder einen Sonderweg einzuschlagen, sollte das Schweizer Datenschutzgesetz die Busshöhen für Datenschutzverstösse an die EU-Verordnung angleichen.

5. Präzisierung des Begriffs „geheime Personendaten"

Der Begriff „geheime Personendaten" in Art. 52 VE-DSG muss präzisiert werden.

Der in Art. 52 festgehaltene Ausbau der Schweigepflicht stellt jede unbefugte Offenlegung von geheimen Personendaten unter Strafe. Jedoch wird im Gesetzesentwurf der Begriff „geheime Personendaten" nicht präzisiert womit entscheidend sein wird, wie die Begrifflichkeit ausgelegt wird. Dies kann durch eine verständliche Präzisierung vermieden werden.

Kontakt: Dr. Matthias Stürmer, Geschäftsleiter Parlamentarische Gruppe Digitale Nachhaltigkeit Parldigi
info@digitale-nachhaltigkeit.ch, www.digitale-nachhaltigkeit.ch

patronfonds
Unternehmerische Verantwortung in der 2. Säule

patronfonds c/o furrerhugi. AG | Schauplatzgasse 39 | CH-3011 Bern +41 31 313 18 48 | info@patronfonds.ch
per email an: jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement
Frau Bundesrätin Simonetta Sommaruga
Bundeshaus West
CH-3003 Bern

Bern, 4. April 2017

Vernehmlassung zum Vorentwurf (VE) zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG)

Sehr geehrte Frau Bundesrätin Sommaruga, sehr geehrte Damen und Herren

Mit Schreiben vom 21. Dezember 2016 haben Sie interessierte Kreise zur Vernehmlassung zum Vorentwurf über die Totalrevision des Datenschutzgesetzes eingeladen.

PatronFonds ist ein Verband der patronalen Wohlfahrtsfonds mit Ermessensleistungen und Finanzierungsstiftungen (www.patronfonds.ch). Er setzt sich für die Interessen seiner Mitglieder und insbesondere für bessere Rahmenbedingungen ein.

Gerne machen wir von der Möglichkeit Gebrauch, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE DSG) eine kurze Vernehmlassung einzureichen.

1. Zu den Wohlfahrtsfonds / unbefriedigende datenschutzrechtliche Grundlage

Wohlfahrtsfonds mit und ohne reglementarische Leistungen qualifizieren als Einrichtungen der beruflichen Vorsorge (vgl. Art. 89a Abs. 6 und 7 ZGB, in Kraft seit 1. April 2016). Die Revision von Art. 89a ZGB hatte bekanntlich zum Ziel, Wohlfahrtsfonds ohne reglementarische Leistungen1 zu stärken, sie administrativ zu entlasten und die Rahmenbedingungen zu verbessern (vgl. Parlamentarische Initiative Pelli, 11.457 / Art. 89a Abs. 7 und 8 ZGB). Die sozialpolitisch wichtige Bedeutung von Wohlfahrtsfonds ist vom Gesetzgeber und ganz allgemein anerkannt (vgl. z.B. BGE 137 V 321).

Patronale Wohlfahrtsfonds sind steuerbefreite, im Unterschied zu den Pensionskassen aber nicht registrierte Einrichtungen der beruflichen Vorsorge, die somit nicht an der Durchführung der obligatorischen Vorsorge beteiligt sind. Datenschutzrechtlich gelten sie damit im Unterschied zu den Pensionskassen wohl als private Personen (vgl. BVGer A-4467/2011 vom 12. April 2012, E. 4.2.).

Ermessensleistungen von Wohlfahrtsfonds sind dem Grundkonzept der beruflichen Vorsorge (Alter, Tod und Invalidität) verhangen und können traditionell auch bei Krankheit, Unfall und Arbeitslosigkeit in Notlagen ausgerichtet werden.

Konkret erbringen Wohlfahrtsfonds mit Ermessensleitungen vielfältige Härtefallleistungen im Einzelfall (z. B. Finanzierung einer Zahnarztrechnung, Unterstützung von behinderungsgerechten Massnahmen, Ermöglichung einer vorzeitigen Pensionierung in einem Härtefall etc.). Sie haben dabei sinngemäss die Grundsätze der Angemessenheit und der Gleichbehandlung der Destinatäre zu berücksichtigen (Art. 89a

1 insbesondere Wohlfahrtsfonds mit Ermessensleistungen und Finanzierungsstiftungen.

Abs. 8 Ziff. 3 ZGB). Sie können traditionell auch bei der Ausgestaltung von Sozialplänen von den Sozialpartnern beigezogen werden. Im Teil- oder Gesamtliquidationsfall, aber auch bei einer freiwilligen Verteilung von freien Mitteln, haben sie Verteilpläne für ihre Destinatäre zu erstellen. Zur Erfüllung ihrer vorsorgerechtlichen Aufgaben sind sie zwangsläufig auf sensible Daten wie Lohn, Alter, Dienstalter, Vorsorgeguthaben etc. angewiesen. Dies gilt auch für die Wohlfahrtsfonds mit reglementarischen Leistungen (Art. 89a Abs. 6 ZGB).

Wohlfahrtfonds mit und ohne reglementarische Leistungen müssen ihre statutarischen vorsorgerechtlichen Aufgaben unbürokratisch und rasch auf einer klaren datenschutzrechtlichen Grundlage erfüllen können. Auch wenn sie als "private Personen" für die Bearbeitung von Daten nicht von vornherein über eine gesetzliche Grundlage wie die Pensionskassen verfügen müssen, wäre eine datenschutzrechtliche Klarstellung mittels gesetzlicher Grundlage bereits heute sehr zu begrüssen. Dies gilt umso mehr, als in Art. 23 Abs. 2 in Verbindung mit Art. 3 Bst. f VE DSG bei der Persönlichkeitsverletzung auch das Profiling aufgeführt wird. Art. 24 Abs. 1 VE DSG (bzw. Art. 13 DSG) nennt denn – allerdings nur als blossen "Rechtfertigungsgrund" – auch eine Rechtfertigung durch Gesetz.

Art. 85a Bst. b BVG hält unter dem Titel *"Bearbeiten von Personendaten"* für Pensionskassen unter anderem folgendes fest:
"Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:
…
b. Leistungsansprüche zu beurteilen sowie Leistungen zu berechnen, zu gewähren und diese mit Leistungen anderer Sozialversicherungen zu koordinieren;
…"
Diese Bestimmung kann auch für Wohlfahrtsfonds mit und ohne reglementarische Leistungen als Rechtsgrundlage herangezogen werden.

PatronFonds **beantragt** deshalb eine **Änderung von Art. 89a Abs. 6 Ziff. 5a und Art. 89a Abs. 7 Ziff. 2 ZGB**, indem der **Verweis auf Art. 85a Bst. b BVG** in das ZGB aufgenommen und der Verweisungstext durch **"Bearbeiten von Personendaten"** entsprechend ergänzt wird. Dies umso mehr, als der VE DSG schon fahrlässige Verstösse gegen das DSG massiv sanktionieren will. Denkbar wäre auch ein entsprechender Verweis auf Art. 85a Bst. b bis f BVG.

Die Rechtslage bleibt für Wohlfahrtsfonds mit und ohne reglementarische Leistungen unbefriedigend und mit Rechtsunsicherheiten behaftet. Für Rückfragen oder ein diesbezügliches vertiefendes Gespräch stehen wir gerne zur Verfügung.

2. Zum VE DSG

Wie dargelegt, werden Wohlfahrtsfonds mit und ohne reglementarische Leistungen vom totalrevidierten Datenschutzgesetz betroffen sein. Viele dieser Einrichtungen sind kleine Institutionen ohne nennenswerte Personalressourcen. Die Anwendung des geplanten neuen Datenschutzgesetzes wird zahlreiche Wohlfahrtsfonds mit seiner Komplexität überfordern, was wiederum Folgen für den Fortbestand dieser Institutionen haben kann. Wir bedauern dies. Es gilt, eine Überregulierung zu vermeiden.

Wir vertreten die Auffassung, dass das bestehende Datenschutzgesetz genügt. Dessen Umsetzung ist effizienter und kostengünstiger, als es beim neuen Gesetz der Fall wäre. PatronFonds hat aber auch ein gewisses Verständnis dafür, dass die Schweiz das revidierte europäische Recht (Übereinkommen SEV 108; EU-Datenschutzgrundverordnung) nachvollziehen will, ist aber strikte dagegen, über die Anforderungen der EU hinauszugehen. Nachfolgend erlauben wir uns kurze Bemerkungen zu einzelnen vorgesehenen Regelungen:2

Das **Profiling (Art.3 lit. f VE DSG)** ist sehr weit und soll ohne ausdrückliche Einwilligung der betroffenen Personen *per se* persönlichkeitsverletzend sein (vgl. Art. 23 Abs. 2 lit. d E-DSG). Letztere Regelung halten

2 PatronFonds verweist diesbezüglich auch auf die eingehendere Vernehmlassung von ProFonds, Dachverband gemeinnütziger Stiftungen in der Schweiz, vom 4. April 2017.

wir für massiv übertrieben und **beantragen** entsprechend eine ersatzlose Streichung. Der Begriff "Profiling" ist demgegenüber angemessen einzuschränken.

Die **Datenschutz-Folgeabschätzung (Art. 16 VE DSG)** erachten wir ebenfalls als problematisch und für kleinere Einrichtungen im Verhältnis zum Nutzen der Folgeabschätzung als zu aufwändig.

Als zu weit gehend erachten wir die in **Art. 17 VE DSG** normierte **Meldung von Verletzungen des Datenschutzes**. Solche Datenschutzverletzungen dürften in der Praxis häufig vorkommen. Eine Meldepflicht ist unangebracht, namentlich unter dem Aspekt der scharfen Strafdrohung bei Verletzung der Meldepflicht (vgl. Art. 50 Abs. 2 lit. e VE DSG). Wir **beantragen** deshalb eine Reduktion der Meldepflicht auf ein vernünftiges Mass, mindestens auf das Niveau der EU. Generell sind Melde- und Informationspflichten auf das Notwendige zu reduzieren.

Als nicht zielführend erachten wir im Weiteren die **Strafbestimmungen (Art. 50 ff. VE DSG).** Das geltende DSG kennt von der Übertretungsnorm gemäss Art. 34 DSG abgesehen keine nennenswerten Strafbestimmungen. Die neuen Strafbestimmungen von Art. 50 ff. VE DSG richten sich gegen private Personen. Erfasst werden auch fahrlässige Datenschutzverstösse. Dies führt letztlich zu einer stossenden Kriminalisierung von Organen und Mitarbeitern. Die Bussenobergrenze von CHF 500'000 (für vorsätzliche Tatbegehung) und CHF 250'000 (für fahrlässige Tatbegehung) ist massiv. Fraglich ist zudem, ob die Strafbestimmungen den strafrechtlichen Prinzipien wie dem Selbstbelastungsverbot, dem Bestimmtheitsgebot und dem Verschuldensprinzip genügen. Abzulehnen ist auch die Einführung einer neuen beruflichen Schweigepflicht in Art. 52 VE DSG, deren Missachtung mit einer Freiheitsstrafe bis zu drei Jahren pönalisiert ist. Wir **beantragen**, die Strafbestimmungen zu überarbeiten und sie hinsichtlich Anwendungsbereich und Sanktionshöhe auf ein vernünftiges Mass zu reduzieren. Fahrlässigkeitsdelikte sind ersatzlos zu streichen.

Zur geplanten Änderung von Art. 81a BVG Einleitungssatz: Nicht ersichtlich ist, weshalb darin der Begriff "Persönlichkeitsprofile" ersatzlos gestrichen werden soll. Einrichtungen der beruflichen Vorsorge sehen sich relativ rasch gezwungen, für ihre Aufgaben Daten im Sinne des im VE DSG definierten Begriffs "Profiling" zu bearbeiten. Wir **beantragen,** den Begriff der Persönlichkeitsprofile in **Art. 85a VE BVG** durch **Profiling** zu ersetzen (sofern das Profiling neu eingeführt wird)**.** Andernfalls wäre in der Definition von Art. 3 Bst. f VE DSG zu klären, dass die "schützenswerten Daten" auch das Profiling umfassen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Berücksichtigung unserer Anträge und stehen für allfällige Rückfragen jederzeit zur Verfügung.

Freundliche Grüsse

PatronFonds

Yolanda Müller
Vorstandsmitglied

Lorenz Furrer
Geschäftsführer

Amstutz Jonas BJ

Von: Stefan Isliker <sisliker@pdc-online.com>
Gesendet: Freitag, 31. März 2017 11:29
An: Amstutz Jonas BJ
Cc: Hans Peter Popp
Betreff: pdc: Stellungnahme / Vernehmlassung DSG
Anlagen: Vernehmlassung_VE DSG_pdc Marketing_v 2.0_30032017.doc

Wichtigkeit: Hoch

Sehr geehrter Herr Amstutz

Im attachment senden wir Ihnen die Stellungnahme der pdc Gruppe (pdc Marketing + Information Technology AG ff) für den Vorentwurf zur Vernehmlassung DSG.

Besten Dank für die Bestätigung und Berücksichtigung.

Datenschutzbeauftragter: Hanspeter Popp
VRP/CEO Stefan Isliker

Freundliche Grüsse aus Wettingen
Stefan Isliker
CEO

pdc Marketing + Information Technology AG
> Agentur für Kundenmanagement <
Schwimmbadstrasse 45
5430 Wettingen
Schweiz

Telefon +41 56 437 88 55
Direktwahl +41 56 437 88 51
Telefax +41 56 437 88 35
Mobil +41 79 448 22 12

Member of FullSolution
Internet www.pdc-online.com

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : pdc Marketing und Information Technology AG

Abkürzung der Firma / Organisation : pdc

Adresse : Schwimmbadstrasse 45, 5430 Wettingen

Kontaktperson : Stefan Isliker

Telefon : 056 437 88 55

E-Mail : sisliker@pdc-online.com

Datum : 31. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
pdc	Wir begrüssen die Modernisierung des Datenschutzrechts im Grundsatz. Es ist wichtig, dass die Gesetzgebung die technologischen Entwicklungen berücksichtigt. Im Zusammenhang mit der Digitalisierung der Wirtschaft wird die Bearbeitung von Personendaten ein immer wichtigeres Thema werden. Aus Sicht von pdc ist bei der Regulierung des Datenschutzrechts auch die Entwicklung im Ausland zu beachten. Einerseits werden bei der globalen Vernetzung der schweizerischen Wirtschaftsunternehmen regelmässig Personendaten grenzüberschreitend transferiert. Andererseits stehen die schweizerischen Unternehmen regelmässig in Konkurrenz mit ausländischen Unternehmen. Die Gesetzgebung kann in diesem Wettbewerb ein Standortvor- oder –nachteil bedeuten. Für pdc war die liberale Ausgestaltung des schweizerischen Datenschutzrechts bis anhin ein Standortvorteil. Die Kunden von pdc könnten ihre Datenbearbeitungen auch jederzeit bei einem anderen, ausländischen Dienstleister durchführen lassen. An diesem Standortvorteil darf nicht gerüttelt werden. Praktisch alle Dienstleistungen, welche pdc, gegenüber deren Kunden erbringt, basieren auf Datenbearbeitungen. Korrekte Datenbearbeitungen und Datensicherheit sind daher für pdc geschäfts-relevante Themen. Aus Sicht von pdc ist bei der Regulierung von Datenbearbeitungen ein Ausgleich zwischen den Interessen der betroffenen Personen und der Datenbearbeiter besonders wichtig. pdc unterstützt Unternehmen, die vor allem aus der Automobil-Industrie stammen, im Zusammenhang mit Unternehmens-, Marketing- und IT-Beratung sowie Marktforschung. pdc ist hierbei einer der grössten Marktteilnehmer und zählt namhafte, auch ausländische Automobil-Hersteller, wie auch kleinere Autohändler zu seinen Kunden. pdc entwickelt und stellt den Unternehmen auch die für die Umsetzung von Marketingstrategien und –aktivitäten notwendigen Tools zur Verfügung (z.B. CRM-Applikationen, Analysetools, Datenbank-Tools, etc.). pdc agiert bei allen diesen Dienstleistungen als Auftragsbearbeiter. Gleichwohl ist pdc daran interessiert, dass die datenschutzrechtlichen Pflichten für die Verantwortlichen verhältnismässig und umsetzbar sind. Müssen die Verantwortlichen, d.h. die Kunden von pdc, Datenbearbeitungen einschränken, trifft dies die Dienstleistungen von pdc direkt. In der heutigen Wirtschaftslage, in welcher insbesondere schweizerische Unternehmen, inklusive KMUs, unter einem erhöhten Wettbewerbsdruck stehen, ist die zielgerichtete, individualisierte und interessengeleitete Kommunikation mit bestehenden Kunden enorm wichtig. Die Kunden haben eine grosse Auswahl und die Brandloyalität kann schnell abnehmen. Zudem ist es für den wirtschaftlichen Erfolg von Unternehmen besonders wichtig, neue Kunden zu gewinnen. Dafür benötigen die Unternehmen Adressen von potenziellen neuen Kunden. pdc unterstützt deren Kunden auch bei dieser Aufgabe. Zusammenfassend erbringt pdc für deren Kunden Aufgaben und Dienstleistungen, welche im heutigen, verschärften Wettbewerb besonders wichtig sind. Die Dienstleistungen von pdc sind auch für die Konsumenten sehr wichtig. Die Dienstleistungen ermöglichen es den pdc-Kunden die Konsumenten mit grösster Professionalität zu betreuen und die Bedürfnisse der Konsumenten umfassend zu befriedigen. pdc steht bei diesen Dienstleistungen in einem strengen Wettbewerb mit in- und vor allem auch ausländischen Dienstleistern. Gleich lange Spiesse

	bei der Datenbearbeitung sind daher für pdc (und deren Kunden) von erheblicher Bedeutung. Aufgrund der vorangehenden Ausführungen lehnen wir jeglichen Swiss Finish strikte ab. Für pdc ist es wichtig, dass das Datenschutzrecht im Vergleich zu ausländischen Regeln weiterhin einem liberalen Ansatz folgt. Wir sind uns bewusst, dass die Schweiz verpflichtet ist, die Vorgaben der Europarats-Konvention (E-SEV 108) umzusetzen. Dabei ist jedoch zu beachten, dass diese Vorgaben durchaus Umsetzungsspielraum bieten. Betreffend die EU-Datenschutzgrundverordnung reicht es aus, wenn die schweizerische Regelung als angemessen qualifiziert werden kann. Hierfür ist keine eins-zu-eins Umsetzung notwendig. Schon gar nicht darf die schweizerische Regelung über die Vorgaben der EU-DSGVO hinausgehen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
pdc	DSG	1			Die „Förderung des freien Verkehrs von Personendaten“ ist in die Zweckbestimmung aufzunehmen.
pdc	DSG	3		a	pdc begrüsst, dass sich der Begriff „Personendaten“ inhaltlich nicht ändern soll. Verwirrend sind hierzu die Ausführungen im erläuternden Bericht. Es wird dort aus Erwägungsgründen zur EU-DSGVO zitiert. Die betreffenden Erwägungen haben jedoch nachgerade in Deutschland für Verwirrung gesorgt. Aus Sicht von pdc sollte in den Materialien, d.h. in der Botschaft, ausschliesslich auf die Praxis und Rechtsprechung zum geltenden DSG verwiesen werden. Klarzustellen ist explizit, dass für die Frage der Bestimmbarkeit die sog. relative Methode massgebend ist.
pdc	DSG	3		f	**Bei dieser Definition des Profiling handelt es sich um einen Swiss Finish. Darauf ist zu verzichten.** Der Begriff Profiling ist zunächst auf das automatisierte Profiling zu beschränken. Dies entspricht der Regelung in der EU-DSGVO. Zu streichen ist auch die Unterscheidung zwischen Personendaten und Daten. Dies sorgt unnötig für Verwirrung. Zuletzt mangelt es an einer für die Praxis brauchbaren Präzisierung, wann genau ein Profiling vorliegt. Die Ausführungen im erläuternden Bericht helfen hier nicht weiter. Die Ausführungen führen zu einem praktisch uferlosen Profiling-Begriff. Nicht jede Auswertung führt jedoch bei der betroffenen Person zu einem erhöhten Schutzbedürfnis. Bereits nach geltendem Recht war beim Persönlichkeitsprofil nicht jede Zusammenstellung von Personendaten, welche wesentliche Teile der

					Persönlichkeit abbildeten, ein Persönlichkeitsprofil im Sinne des DSG. Um ein konkretes Beispiel zu nennen. Es wird erwähnt, dass Auswertungen betreffend die wirtschaftliche Lage ein Profiling sein können. Bei der Selektion von Adressdaten für Kundenkommunikation wird hierzu regelmässig auch die Kaufkraft als Variable verwendet. Die Kaufkraft wäre ein Merkmal für die wirtschaftliche Lage. Die Kaufkraft lässt sich nun auf verschiedene Arten bestimmen. Verfügt ein Unternehmen z.B. über Transaktionsdaten lässt sich die Kaufkraft anhand dieser Daten über einen längeren Zeitraum bestimmen. Die Kaufkraft kann jedoch auch anhand von relativ statischen Informationen, z.B. der Wohngemeinde, dem Alter, dem Beruf, etc., berechnet werden. Die so errechnete Kaufkraft gibt ein ganz anderes Bild über die Persönlichkeit der betreffenden Person ab als die anhand von Transaktionsdaten berechnete Kaufkraft.
pdc	DSG	4			pdc begrüsst, dass das geltende Konzept der Datenbearbeitungsgrundsätze beibehalten wird. Wichtig ist aus Sicht von pdc, dass das grundsätzliche Konzept des schweizerischen Datenschutzrechts sich nicht ändert. In der Schweiz sind Datenbearbeitungen bei Einhaltung der Datenbearbeitungsgrundsätze erlaubt und es wird weder eine Einwilligung noch ein anderer Rechtfertigungsgrund benötigt, sofern dies im Gesetz nicht explizit verlangt wird. In der EU gilt der Grundsatz des Verbotes mit Erlaubnisvorbehalt, d.h. jede Datenbearbeitung muss gerechtfertigt werden. Das schweizerische Grundkonzept entspringt dem schweizerischen liberalen Gedankengut, welches auf den mündigen, eigenverantwortlichen Bürger abstellt. Dieses liberale Gedankengut ist beizubehalten.
pdc	DSG	4	3		Die Voraussetzung der „klaren“ Erkennbarkeit ist zu streichen. Gemäss erläuterndem Bericht ist zu Recht keine inhaltliche Änderung beabsichtigt. Der Bezug auf eine „klare“ Erkennbarkeit verwirrt daher nur.
pdc	DSG	4	5		Gemäss erläuterndem Bericht sind keine Änderungen an der geltenden Regelung beabsichtigt. Daher erachten wir es auch nicht als notwendig, den Wortlaut zu

					ändern. Diese Änderung führt nur zu Verwirrung und Rechtsunsicherheit.
pdc	DSG	4	6		**Es ist unklar, weshalb der Wortlaut geändert wird, obwohl gemäss erläuterndem Bericht explizit keine inhaltliche Änderung geplant ist.** Die Änderung des Wortlautes führt unnötig zu Verwirrung. Der Wortlaut sollte auch deshalb nicht geändert werden, weil in der EU-DSGVO aus dem vergleichbaren Wortlaut sehr strenge Anforderungen an die Einwilligung herausgelesen wurden. Solche inhaltlichen Änderungen sind gerade nicht geplant. In den Materialien ist explizit klarzustellen, dass sich an den Anforderungen an die Einwilligung im bisherigen Recht nichts ändert. Die strengen Anforderungen in der EU-DSGVO werden explizit nicht übernommen. Zuletzt ist der Begriff der ausdrücklichen Einwilligung nicht klar. In den Materialien ist der Begriff noch besser zu erklären.
pdc	DSG	5+6			**Bei den Regelungen zur Bekanntgabe von Daten ins Ausland handelt es sich um einen Swiss Finish. Auf diesen ist zu verzichten.** Zur Einhaltung der E-SEV 108 ist unseres Erachtens keine inhaltliche Änderung der Datentransfer-Regelung notwendig. Auch die EU-DSGVO bzw. die Sicherstellung der Angemessenheit zum betreffenden Datenschutzstandard verlangt keine solch komplizierte Umsetzung. Unnötig – und auch durch die EU-DSGVO nicht gefordert – ist die generelle Informationspflicht bei der Nutzung von standardisierten Garantien (Art. 5 Abs. 6 VE-DSG). Zuletzt ist in Art. 6 Abs. 1 lit. a VE-DSG der Zusatz „im Einzelfall“ zu streichen. Bei wiederkehrenden Sachverhalten und unveränderter Erkennbarkeit und Erwartung muss eine einmalige Zustimmung ausreichen.

pdc	DSG	7			**Auch bei der vorgeschlagenen Regelung zur Auftragsbearbeitung handelt es sich um einen Swiss Finish.** Zur Einhaltung des E-SEV 108 reicht die heute geltende Regelung aus. Die Anforderungen an den Beizug von Subunternehmern führen im wirtschaftlichen Alltag zu unnötigen Beeinträchtigungen, ohne dass dadurch der Schutz für die betroffenen Personen erhöht würde. Für die betroffenen Personen ist entscheidend, dass der Verantwortliche für alle Auftragsdatenbearbeitungen letztverantwortlich bleibt. Zuletzt ist die unbeschränkte Delegation zur Festlegung weiterer Pflichten an den Bundesrat zu streichen. Die Anforderungen an die Auftragsdatenbearbeitung sind bereits nach geltendem Recht ausreichend. Die Kompetenz an den Bundesrat ist damit nicht notwendig.
pdc	DSG	8			pdc begrüsst die Einführung von Empfehlungen der guten Praxis. Dies ist wichtig, um die teilweise unbestimmten Artikel mit Leben und Präzisierungen zu erfüllen. Unseres Erachtens muss jedoch die Initiative für solche Empfehlungen ausschliesslich von den Verbänden oder Branchenorganisationen kommen. Der EDÖB darf kein Recht zum Erlass von Empfehlungen erhalten. Er kann jedoch durchaus beratend tätig werden. Zuletzt ist gegen Entscheide betreffend die Genehmigung oder Nicht-genehmigung von Empfehlungen der guten Praxis ein Rechtsmittel zur Verfügung zu stellen. In den Materialien sind die Voraussetzungen für dieses Rechtsmittel, insbesondere die Beschwerdelegitimation genauer darzulegen.
pdc	DSG	13			Es ist fraglich, ob eine allgemeine aktive Informationspflicht bei allen Datenbearbeitungen aus Sicht der Transparenz einen Mehrwert bringt. Die allgemeine Informationspflicht entspricht auch nicht dem risiko-basierten Ansatz. Wichtig ist bei der Informationspflicht, dass in den Materialien explizit klargestellt

					wird, dass sich hieraus keine Pflicht zur Nachinformation ergibt. Die Informationspflicht muss im Zeitpunkt der Datenbeschaffung erfolgen und die Informationen beinhalten, die in diesem Zeitpunkt bekannt sind. Ändern sich die betreffenden Informationen, ergibt sich, zumindest aus Art. 13 VE-DSG, keine neue Informationspflicht. Wichtig ist auch eine Klarstellung betreffend die Umsetzung der Informationspflicht. Wie bis anhin muss es zulässig sein, dass die Information mittels standardisierter Datenschutzerklärungen auf der Webseite erfolgt. Dies wird auch durch den E-SEV 108 explizit erlaubt.
pdc	DSG	13	2		Die Auflistung der Informationen, welche bekannt gegeben werden müssen, muss abschliessend sein. Sonst ergeben sich Rechtsunsicherheiten, welche mit Blick auf die Sanktionsandrohung problematisch sind.
pdc	DSG	13	4		**Es handelt sich um einen Swiss Finish**. Die Regelung ist zu streichen.
pdc	DSG	13	5		Die Ausdehnung der Pflicht auf die indirekte Datenbeschaffung wird in der Praxis jegliche Beschaffung von Daten bei Dritten verunmöglichen. Die Bestimmung ist zu streichen. Sollte an dieser Pflicht festgehalten werden, ist, wie in der EU-DSGVO, klar zustellen, dass die Information auch später, z.B. im Zeitpunkt der ersten Kommunikation mit der betroffenen Person erfolgen darf. Zudem muss klargestellt werden, dass die Information auch hier in standardisierten Datenschutzerklärungen auf der Webseite erfolgen darf.
pdc	DSG	14			**Es handelt sich wiederum um einen Swiss Finish. Darauf ist zu verzichten.** Die EU-DSGVO sieht weitergehende Ausnahmen vor. Diese sind auch ins schweizerische Gesetz zu übernehmen.

pdc	DSG	15			**Auch hier handelt es sich um einen Swiss Finish.** **Es ist explizit klarzustellen, dass auch rechtliche Auswirkungen eine gewisse Schwere erreichen müssen.** Zudem sind, wie in Art. 22 EU-DSGVO, Ausnahmen zur Informationspflicht vorzusehen.
pdc	DSG	16			**Auch bei dieser Bestimmung wurde unnötigerweise ein Swiss Finish eingebaut.** **Der Anwendungsbereich der Pflicht zur Datenschutz-Folgenabschätzung ist gemäss Vorschlag viel zu weit gefasst.** Theoretisch könnte bei diesem Vorschlag jede Datenbearbeitung, z.B. auch eine einzelne Datenbekanntgabe ins Ausland, eine Datenschutz-Folgenabschätzung auslösen. Dies würde zu einer administrativen Überbelastung der Datenbearbeiter und des EDÖB führen. Wie in der EU-DSGVO sollte die Datenschutz-Folgenabschätzung auf Datenbearbeitung mit einem hohen (oder besser sehr hohen) Risiko beschränkt bleiben. Zudem sollte die Folgenabschätzung nur bei Datenbearbeitungen ausgelöst werden, die regelmässig durchgeführt werden. Für eine einmalige Datenbearbeitung soll es keine solche Pflicht geben. **Es ist darauf zu verzichten, dass auch der Auftragsbearbeiter eine solche Datenschutz-Folgenabschätzung durchführen muss.** Dies wird weder durch die EU-DSGVO noch den E-SEV 108 verlangt. Zuletzt ist die Notifkationspflicht an den EDÖB zu ändern. Nach dem jetzigen Vorschlag müsste bei jeder Datenschutz-Folgenabschätzung das Ergebnis an den EDÖB notifiziert werden. In der EU-DSGVO (Art. 36) ist eine Notifikation nur vorgesehen, wenn sich aus der Folgenabschätzung effektiv ein hohes Risiko ergibt und wenn der Datenbearbeiter dieses Risiko nicht durch geeignete Massnahmen reduzieren kann oder will. Diese Regelung ist absolut ausreichend und sollte für die Schweiz übernommen werden.

pdc	DSG	17	1		**Es handelt sich wiederum um einen Swiss Finish. Dies ist zu vermeiden.** Die Meldepflicht an den EDÖB sollte nur dann ausgelöst werden, wenn sich aus einer Datenschutzpanne ein ernsthaftes Risiko für die betroffene Person ergibt. Dies genügt, um den E-SEV 108 einzuhalten.
pdc	DSG	17	2		Diese Pflicht ist zu streichen. Sie ist im E-SEV 108 nicht zwingend vorgesehen.
pdc	DSG	18			Bei diesen neuen Pflichten ist vollkommen unklar, was die Datenbearbeiter genau tun müssen. Der erläuternde Bericht bringt hierzu auch keine Klarstellung. In den Materialien sind konkrete Beispiele aufzuführen, damit sich die Datenbearbeiter von ihren Pflichten eine allgemeine Vorstellung machen können.
pdc	DSG	19		a	**Die Regelung darf keinesfalls über das in der EU-DSGVO (Art. 30) vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgehen.** Damit ein solches Verzeichnis überhaupt seinen Zweck erfüllen kann, muss es jedenfalls auf regelmässige Datenbearbeitungen beschränkt sein. Darüber hinaus sind, wie in der EU-DSGVO vorgesehen (Art. 30 Abs. 5), entsprechende Ausnahmen einzufügen.
pdc	DSG	19		b	**Eine solche Mitteilungspflicht ist im E-SEV 108 nicht vorgesehen. Sie ist damit zu streichen.** Wird an der Pflicht festgehalten, ist sie auf Konstellationen zu beschränken, in denen ein berechtigtes Interesse der betroffenen Person für eine solche Information besteht. Zudem ist der Auftragsbearbeiter aus dem Artikel zu streichen. Die Pflicht soll, wenn überhaupt, nur den Verantwortlichen treffen. Dieser entscheidet letztlich über Datenweitergaben.

pdc	DSG	20	1		**Es handelt sich um einen Swiss Finish, der zu streichen ist.** E-SEV 108 verlangt keine Kostenlosigkeit.
pdc	DSG	20	3		**Beim Auskunftsrecht im Zusammenhang mit automatisierten Einzelfallentscheiden handelt es sich ebenfalls um einen Swiss Finish.** Das Auskunftsrecht ist auf die Konstellationen zu beschränken, in denen eine Informationspflicht besteht. Zudem ist in den Materialien explizit klarzustellen, dass Geschäftsgeheimnisse beim Auskunftsrecht zu berücksichtigen sind.
pdc	DSG	23	2	d	**Diese Regelung stellt einen Swiss Finish dar und führt zu einer unnötigen Erschwerung der personalisierten Kommunikation. Die Regelung ist daher zu streichen.** **Wird diese Vorschrift Gesetz, verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar**. Diese Dienstleistungen würden im Worst Case ins Ausland abwandern bzw. durch Dienstleister im Ausland durchgeführt werden.
pdc	DSG	23	3		pdc begrüsst, dass an dieser bereits geltenden Regelung nichts geändert werden soll. Gerade beim personalisierten Marketing werden regelmässig solche veröffentlichten Daten verwendet.
pdc	DSG	44	3		**Gegen vorsorgliche Massnahmeverfügungen des EDÖB muss es zwingend ein Rechtsmittel mit aufschiebender Wirkung geben.** Solche Massnahmeverfügungen können bei den Datenbearbeitern zu erheblichen Schäden führen. Die Rechtsprechung des Bundesverwaltungsgerichts zeigt, dass immer wieder mal eine solche Verfügung des EDÖB aufgehoben wird.

pdc	DSG	50 ff.			**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt.** Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Die vorgeschlagene Sanktionsregelung führt dazu, dass die für Datenbearbeitungen verantwortlichen Personen in den Unternehmen direkt mit Strafrisiken bedroht sind. Die subsidiäre Haftung des Unternehmens dürfte gerade bei kleineren Unternehmen, wo die verantwortliche Person relativ leicht eruiert werden kann, nicht zur Anwendung gelangen. Die Strafrisiken für die verantwortlichen Personen würden dazu führen, dass kein Mitarbeiter bereit wäre, die Funktion eines internen Datenschutzbeauftragten zu übernehmen. Dies ist aus Sicht der Datenschutz-Compliance negativ. Zudem würde die Strafbarkeit der Mitarbeiter dazu führen, dass diese – allenfalls vorschnell – Verstösse und vermeintliche Verstösse dem EDÖB melden, um sich selber zu entlasten. Die vorgeschlagene Sanktionslösung führt darüber hinaus bei schweizerischen Unternehmen zu Wettbewerbsnachteilen. Die Vollstreckung allfälliger Sanktionen gegenüber ausländischen Unternehmen wäre stark erschwert, weshalb sich diese allenfalls gar nicht an die Regeln halten würden. Des Weiteren verstösst die vorgeschlagene Regelung gegen gewichtige (rechtsstaatliche) strafprozessuale Prinzipien. Betroffen ist primär das Bestimmtheitsgebot. Tangiert ist aufgrund der verschiedenen Informations-, Melde- und Mitwirkungspflichten im VE-DSG jedoch auch der Grundsatz „nemo tenetur“, d.h. das Selbstbelastungsgebot. Die Pflicht, Datenschutzverstösse zu melden, welche ihrerseits strafbedroht ist, führt faktisch zu einer Selbstanzeigepflicht. Betreffend die Ausgestaltung eines alternativen Sanktionssystems verweisen wir auf den entsprechenden Vorschlag der economiesuisse. Im Vordergrund stehen Verwaltungsstrafen gegen das Unternehmen und nicht die natürlichen Personen.

					Anknüpfungspunkt für die Strafbarkeit der Unternehmen wären Organisationsmängel im Unternehmen, d.h. eine mangelhafte Datenschutz-Compliance. Lediglich subsidiär soll eine Strafbarkeit von Mitarbeitern möglich sein, wenn diese absichtlich bzw. mit Vorsatz gegen interne oder gesetzliche Datenschutzregeln verstossen haben. Aus rechtsstaatlichen Überlegungen darf nicht der EDÖB über die Verwaltungssanktionen entscheiden. Die untersuchende bzw. anklagende Behörde soll nicht gleichzeitig die urteilende Behörde sein. Um dieses Problem zu lösen, ist eine neue Entscheidinstanz zu gründen. Das Verhältnis zwischen dieser neuen Behörde und dem EDÖB wäre im DSG zu regeln. Betreffend die Anpassung des Strafkataloges in Art. 50 und 51 VE-DSG wird auf die detaillierten Aufführungen in der Stellungnahme von economiesuisse verwiesen. pdc unterstützt die entsprechenden Vorschläge.
pdc	DSG	52			**Die vorgeschlagene Regelung ist weder durch die EU-DSGVO noch den E-SEV 108 erforderlich und daher zu streichen.** Die Regelung würde die Konzeption des Schweizerischen Datenschutzrechts auf den Kopf stellen. Bis anhin durften „normale“ Personendaten grundsätzlich ohne einen Rechtfertigungsgrund an Dritte weitergegeben werden – sofern auch die anderen Datenbearbeitungsgrundsätze eingehalten wurden. Nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile wurde vermutet, dass die Bekanntgabe an Dritte ohne Zustimmung der betroffenen Person eine Persönlichkeitsrechtsverletzung darstellt. Art. 52 VE-DSG würde diesen Mechanismus auf den Kopf stellen. Obwohl eigentlich der materielle Teil des Datenschutzgesetzes für die Bekanntgabe von normalen Personendaten an Dritte keinen Rechtfertigungsgrund verlangt, würde eine solche Pflicht zumindest bei der Bekanntgabe von „geheimen“ Personendaten über den Umweg der strafbewehrten Schweigepflicht eingeführt werden. Hinzu kommt, dass der Begriff der „geheimen Personendaten“ unklar ist.

pdc	DSG	55			Falls die Regelung beibehalten wird, ist die Verjährungsfrist auf 3 Jahre zu reduzieren.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
pdc	3 lit. a	Die Ausführungen im erläuternden Bericht sind unklar und nicht in die Materialien zu übernehmen. Es wird im erläuternden Bericht aus Erwägungsgründen zur EU-DSGVO zitiert, welche in der EU bereits zu Irritationen geführt haben. Es genügt, wenn in den Materialien auf die Praxis und Rechtsprechung zum geltenden DSG verwiesen wird. Klarzustellen ist dabei insbesondere, dass die sog. relative Methode für die Frage der Bestimmbarkeit massgebend ist.
pdc	3 lit. f	Das Profiling wird im erläuternden Bericht nicht genügend präzisiert. Es sind konkrete Beispiele einzubauen. Zudem ist klarzustellen, dass nicht jede Analyse oder Auswertung betreffend die wirtschaftliche Lage oder weitere Persönlichkeitselemente ein Profiling darstellt.
pdc	4 Abs. 6	**Die Ausführungen zum Begriff der Einwilligung sind nicht vollkommen klar. In den Materialien ist explizit festzuhalten, dass keine inhaltliche Änderung beabsichtigt ist. Es gelten die Anforderungen wie nach geltendem Recht.** Es ist explizit klarzustellen, dass die (strengen) Anforderungen aus der EU-DSGVO nicht gelten. pdc würde es begrüssen, wenn in den Materialien auch klargestellt wird, dass die Einwilligung auch weiterhin zu einem Dokument, das weitere Informationen erhält (z.B. AGB oder Datenschutzerklärung), erteilt werden kann und keine separate Einwilligung notwendig ist.
pdc	8	**In den Materialien ist klarzustellen, dass die Initiative von den Verbänden und Branchenorganisationen ausgehen muss. Der EDÖB soll kein Recht haben, Empfehlungen selber zu erlassen.** Gegen die Genehmigung oder Nicht-Genehmigung von Empfehlungen der guten Praxis ist ein Rechtsmittel vorzusehen. Die Einzelheiten zum Rechtsmittel sind in den Materialien näher zu erläutern.

pdc	13	In den Materialien ist ausdrücklich klarzustellen, dass es keine Pflicht zur Nachinformation gibt. Zudem ist klarzustellen, dass die Information in einer standardisierten Datenschutzerklärung auf der Webseite genügt. Sollte an der Informationspflicht bei der indirekten Datenbeschaffung festgehalten werden, ist klarzustellen, dass die Information mittels standardisierter Datenschutzerklärungen auf der Webseite erfolgen kann. Zudem muss es betreffend den Zeitpunkt der Information einen Spielraum geben. Es muss möglich sein, die Information auf den Zeitpunkt der ersten Kommunikation mit der betroffenen Person zu verschieben.
pdc	15	Es ist in den Materialien klarzustellen, dass auch „rechtliche Auswirkungen“ eine gewisse Schwere aufweisen müssen.
pdc	18	Diese Pflichten sind in den Materialien anhand von konkreten Beispielen näher zu erläutern.
pdc	23 Abs. 3	Die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), ist unzutreffend und daher in der Botschaft klar zu stellen.
pdc	24 Abs. 2	In den Materialien ist explizit darauf hinzuweisen, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
pdc	50 ff	**Betreffend die datenschutzgerechte Ausgestaltung des Sanktionssystems kann auf die Ausführungen zu den betreffenden Bestimmungen verwiesen werden.**
pdc	Seite 88	Übergangsbestimmungen In den Materialien ist klarzustellen, dass die neuen Pflichten keine Rückwirkung haben. Personendaten, welche vor Inkrafttreten der neuen Pflichten korrekt beschafft wurden, dürfen auch weiterhin bearbeitet werden, ohne dass z.B. eine Nachinformation notwendig wäre. Es ist für die Umsetzung aller Pflichten eine Umsetzungsfrist von zwei Jahren vorzusehen. Dies entspricht auch der Regelung in der EU-DSGVO.

Amstutz Jonas BJ

Von: Ivo Bühler <Ivo.Buehler@pharmasuisse.org>
Gesendet: Dienstag, 4. April 2017 10:28
An: Amstutz Jonas BJ
Betreff: pharmaSuisse Stellungnahme zur Totalrevision des Datenschutzgesetzes
Anlagen: pharmaSuisse Stellungnahme Datenschutzgesetz.pdf; pharmaSuisse Stellungnahme Totalrevision-des-Datenschutzgesetzes_de.doc

Sehr geehrte Damen und Herren
Sehr geehrter Herr Amstutz

In der Beilage erhalten sie unsere Stellungnahme als word und pdf Dokument. Bitte melden Sie sich bei mir, falls sie das originalunterzeichnete Dokument benötigen. Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüssen

pharmaSuisse
Schweizerischer Apothekerverband
Ivo Bühler
Mitglied der Geschäftsleitung
Stationsstrasse 12, CH-3097 Bern-Liebefeld
T +41 (0)31 978 58 58, F +41 (0)31 978 58 59
www.pharmasuisse.org, ivo.buehler@pharmasuisse.org

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerischer Apothekerverband

Abkürzung der Firma / Organisation : pharmaSuisse

Adresse : Stationsstrasse 12

Kontaktperson : Ivo Bühler

Telefon : 031 978 58 58

E-Mail : info@pharmasuisse.org

Datum : 4.4.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.
2. Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.
3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
pharmaSuisse	Wir beschränken unsere Stellungnahme auf die wichtigsten Punkte der geplanten Gesetzesrevision. pharmaSuisse ist sich als Akteur im Gesundheitswesen der Wichtigkeit des Datenschutzes bewusst. Gerade im Bereich der Gesundheitsdaten soll besonders auf den Datenschutz geachtet werden. Wir erachten das bestehende Gesetz jedoch als genügende Grundlage um den Schutz besonders schützenswerter Daten zu gewährleisten. Für die Unternehmen resultieren aufgrund der Zunahme des beabsichtigten Bearbeitungs- und Administrationsaufwandes für diverse Handlungspflichten unnötig zusätzlichen Kosten und administrativer Aufwand. Wir lehnen die Revision in der vorliegenden Form deshalb ab. Sie gefährdet u.a. Projekte wie das elektronische Patientendossier, welches schon unter dem bestehenden Recht kaum noch finanzierbar ist. Hier wären vor einer Gesetzesänderung die zusätzlichen Regulierungskosten zu berücksichtigen. Leider fehlt eine solche Kostenschätzung. Die Revision ist auf das Minimum zu beschränken, das notwendig ist, um einen im europäischen Vergleich angemessenen Datenschutz zu gewährleisten und soll sich auf den grenzüberschreitenden Datenaustausch beschränken. Dabei sollen die Datenschutzregeln zwischen Europa und USA (Safe Harbor) als Anhaltspunkt dienen. Weitergehende Massnahmen erachten wir nicht als angemessen. Insbesondere erachten wir eine Übernahme der Regelungen der europäischen Datenschutzverordnung als zu weit gehend, zumal es noch offen ist, ob und wie diese Verordnung in den einzelnen Ländern umgesetzt wird und welche Kosten damit verbunden sind. Im Übrigen verweisen wir auf die Stellungnahme des Schweizerischen Gewerbeverbandes. Wir hoffen, dass Sie unsere Anliegen berücksichtigen können. Mit freundlichen Grüssen
	Fabian Vaucher Präsident Marcel Mesnil Generalsekretär

Post CH AG
Corporate Center
Wankdorfallee 4
3030 Bern

Telefon +41 58 386 66 62
Fax +41 58 667 33 73
www.post.ch

C, Wankdorfallee 4, 3030 Bern

Eidg. Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Datum 4. April 2017
Ihre Nachricht
Kontaktperson Gabriele Marianne Schmid-Strasser
E-Mail gabriele.schmid@post.ch
Direktwahl 058 386 66 62

Stellungnahme der Schweizerischen Post zur Revision des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, im Rahmen der Vernehmlassung zum eingangs erwähnten Gesetzesprojekt Stellung zu nehmen, welches die Revision des DSG, den Bundesbeschluss betreffend die Übernahme der EU-Richtlinie sowie die Modernisierung der Datenschutzkonvention des Europarates in einer Vorlage vereint.

1. Ausgangslage für die Schweizerische Post

Die Digitalisierung verändert alle drei Märkte, in denen die Post aktiv ist (Post, Personenverkehr und Finanzdienstleistungen) fundamental und führt zu zunehmend individualisierten Bedürfnissen von Kundinnen und Kunden. Dies gilt auch für den an und für sich „physischen" Logistikmarkt, welcher durch den zunehmend internationalen Wettbewerb sowie den grenzüberschreitenden Warenverkehr geprägt ist. In seinen strategischen Zielen für die Schweizerische Post 2017-2020 fordert der Bundesrat die Post u.a. dazu auf, moderne Kommunikations- und Logistikbedürfnisse durch die Entwicklung zeitgemässer Angebote insbesondere im Bereich des Informations- und Datenverkehrs abzudecken.

Entsprechend diesem Auftrag sowie den Bedürfnissen unserer Kundinnen und Kunden versteht die Schweizerische Post die digitale Transformation in allen Teilmärkten als Teil ihrer Strategie. Dabei möchten wir über eine grösstmögliche regulatorische Sicherheit in der Weiterentwicklung verfügen. Der verantwortungsvolle Umgang mit schützenswerten Kundendaten ist dabei einer unserer zentralen Werte.

Unsere Strategie korrespondiert dabei mit der vom Bundesrat verabschiedeten Strategie „Digitale Schweiz", welche dazu beitragen will, dass unser Land von der zunehmenden Digitalisierung profitiert und sich als innovative Volkswirtschaft noch dynamischer entwickelt. Um dieses Ziel zu erreichen, soll sich die Wirtschaft gemäss Bundesrat im digitalen Raum möglichst frei entfalten können.

2. Grundsätzliches zum Entwurf

Entgegen der in der bundesrätlichen Strategie geäusserten Absichten enthält der vorliegende Vernehmlassungsentwurf zum neuen Schweizer Datenschutzgesetz (nachfolgend VE-DSG) jedoch nach Meinung der Schweizerischen Post wesentliche Hemmschuhe für eine rasche und freie digitale Transformation.

Die Post möchte die Gelegenheit nutzen, im Rahmen des Vernehmlassungsverfahrens folgende vier Hauptkritikpunkte bzw. Anpassungsvorschläge zu deponieren:

Verhältnismässige und praktikable Informations- und Meldepflichten
Die umfassenden Informations- und Meldepflichten führen zu einem massiven administrativen Zusatzaufwand, der mit den aktuellen Ressourcen nicht zu bewältigen wäre. Der zentrale Treiber der digitalen Transformation, nämlich die Entwicklung neuer Produkte, würde künftig durch die verschiedenen Meldepflichten massiv verzögert. **Wir regen deshalb an, die freiwillige Rolle der Datenschutzbeauftragten Person für eine Firma erneut gesetzlich einzuführen und an diese Rolle Erleichterungen betreffend Mitteilungs- und Informationspflichten gegenüber dem EDÖB zu knüpfen.**

Keine „Swiss Finish"-Regelungen
Der Entwurf enthält viele Regelungen aus der DSGVO, welche zusätzlich mit eigenständigen Schweizer Lösungen / Formulierungen ergänzt wurden, so dass in einigen Punkten von den Unternehmungen mehr verlangt wird, als dies aufgrund der internationalen Vorgaben nötig wäre. Insbesondere die verschiedenen Melde- und Informationspflichten gehen über das Notwendige hinaus und generieren einen administrativen Mehraufwand, der den betroffenen Personen keinen zusätzlichen Schutz gewährleistet und deshalb unverhältnismässig ist. Auch die neue Begriffsdefinition des „Profiling" wie auch die besonders schützenswerten Personendaten sollten analog den europäischen Regelungen vorgenommen werden. **Diese „Swiss Finish" - Regelungen sind nicht notwendig, bringen zusätzliche Unklarheiten im Verhältnis zum Europäischen Recht in der Umsetzung und sind daher zu korrigieren.** Zudem muss auch innerhalb der Schweizer Gesetzgebung auf Bundesebene die konsistente Verwendung der Begrifflichkeiten gewährleistet sein.

Verhältnismässiges Sanktionsregime
Zudem erscheint es uns wenig geeignet, DSG-Verletzungen gemäss den im Entwurf definierten Sanktionen zu ahnden. Der VE-DSG zielt auf strafrechtliche Sanktionen gegen die einzelnen Mitarbeitenden persönlich, wobei auch eine fahrlässige Begehung mit hohen Bussen geahndet werden kann. Diese persönlichen Sanktionen gehen über die Regelung in der EU hinaus und sind daher zu korrigieren. **Wir regen an, zu prüfen, ob dem EDÖB die Kompetenz erteilt werden kann, Verwaltungssanktionen auszusprechen**.

Die Förderung der Schweizer Wirtschaft hin zu einer digitalen Schweiz muss stärker in den Fokus des Gesetzesentwurfes
Zusammenfassend gewichtet der Vernehmlassungsentwurf den umfassenden Schutz der Persönlichkeit der betroffenen Personen unverhältnismässig stark, bzw. sieht von einem wirtschaftsfreundlichen, risikobasierten Ansatz ab. Damit wird die Chance verpasst, für die Schweizer Wirtschaft ein Gesetz zu formulieren, welches ihr Freiheiten im Umgang mit neuen, digitalen Technologien ermöglicht und den betroffenen Kunden und den Firmen gleichzeitig die notwendige Rechtssicherheit für einen sicheren Umgang mit Daten gibt.

3. Im Einzelnen

Die Schweizerische Post ist Mitglied des Vereins Unternehmensdatenschutz sowie von SwissHoldings und unterstützt deren Eingaben.

Bezogen auf unseren gesetzlichen Auftrag sowie unsere Tätigkeiten möchten wir zu den folgenden Artikeln aus Sicht der Schweizerischen Post ergänzend zu den bereits erwähnten Eingaben im Detail kurz Stellung beziehen.

Art. 3 VE- DSG:

- *lit. c: Erweiterung der besonders schützenswerten Personendaten um genetische und biometrische Daten:*

Biometrische Daten sollten nur dann besonders schützenswert sein, wenn diese *zum Zweck der Identifizierung* bearbeitet werden, andernfalls wäre bereits jedes Bild/jede Fotografie, auf dem eine Person erkennbar ist, besonders schützenswert.

Erfasst von der Definition in Art. 3 lit. c Ziffer 4 VE-DSG sollten daher nicht biometrische Daten sein, welche eine natürliche Person eindeutig identifizieren, sondern nur solche, die zu diesem Zweck bearbeitet werden, analog der Regelung im E-SEV 108.

Zudem fehlt eine Definition für den neuen Begriff der *„genetischen Daten"*. Genetische Daten werden bei zahlreichen Identifikationssystemen verwendet, so dass eine klare Definition Rechtssicherheit bieten würde.

- *lit. f: neuer Begriff des Profiling:*

Wir unterstützen die Streichung des Begriffes des Persönlichkeitsprofils und die Einführung des neuen Begriffs „Profiling".

Die Definition des Begriffs *Profiling* umfasst jede „Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität". Diese Definition ist aktuell jedoch viel zu breit und geht insbesondere auch weiter als die Definition in der DSGVO. Eine solche weitergehende Definition bedeutet in der Praxis viel Aufwand und führt - insbesondere aufgrund der damit verbundenen Strafbestimmungen und Bussen – zu erheblichen Risiken. Wir empfehlen den Begriff für die Schweiz analog der europäischen Idee zu definieren.

Im VE-DSG fallen unter den Begriff auch Auswertungen von Hand, so dass bereits jede Selektion von Personendaten unter Beizug von nicht personenbezogenen Daten ein Profiling wäre, welches eine Persönlichkeitsverletzung darstellt, sofern nicht vorgängig die ausdrückliche Einwilligung eingeholt wurde.

Die Definition sollte daher auf *automatisierte Auswertungen* eingeschränkt werden, damit nicht jede Handlung unter den Begriff Profiling fällt. Zudem bedarf es einer Klarstellung, wonach das Profiling nur dann vom DSG erfasst ist, *wenn Personendaten vorliegen oder Personendaten entstehen*. Die Analysen von Sachdaten fällt nicht unter den Anwendungsbereich des DSG, weshalb die Formulierung auf Personendaten einzuschränken ist.

Art. 4 VE – DSG: Grundsätze

- *Abs. 6 Einwilligung*

Wir befürworten einen risikobasierten Ansatz auch für die Einwilligungen, d.h. je einschneidender die Folgen sind, desto klarer sollte die Einwilligung erfolgen.

Der Entwurf definiert die *Einwilligung* abweichend von der üblichen zivilrechtlichen Verwendung. Insbesondere die Unterscheidung zwischen einer *eindeutigen und ausdrücklichen Einwilligung erscheint uns nicht schlüssig.*

Die Schweizerische Post betreibt insbesondere im Rahmen ihres Grundversorgungsauftrages ein sehr spezifisches Massengeschäft, welches sich nur sinnvoll abwickeln lässt mit entsprechenden Möglichkeiten in den AGB. Damit die Post auch künftig die Möglichkeit hat, in ihrem spezifischen Massengeschäft Einwilligungen einzuholen, muss eine *„ausdrückliche" Einwilligung auch in den AGB möglich sein*, was aufgrund der Ausführungen in den Erläuterungen jedoch – unseres Erachtens fälschlicherweise – ausgeschlossen wird.

Das Schutzbedürfnis beim Profiling erfordert zudem keine ausdrücklichen Einwilligung. Eine ausdrückliche Einwilligung sollte nur bei besonders schützenswerten Daten notwendig sein.

Art. 6 VE – DSG: Bekanntgabe ins Ausland in Ausnahmefällen

- *Abs. 2 Mitteilungspflicht an EDÖB*

Die in Absatz 2 festgehaltene *Pflicht zur Information des Beauftragten* ist neu und führt zu einem grossen administrativen Mehraufwand. Der Beauftragte wird mit solchen Informationen überhäuft werden und nicht in der Lage sein, diese zu bearbeiten. Zudem ist diese Pflicht dem EU Recht fremd und daher *zu streichen*.

Art. 13 VE-DSG: Informationspflicht bei der Beschaffung von Personendaten

- *Abs. 4: Informationspflicht gegenüber betroffenen Personen, wenn ein Dritter (Auftragsdatenbearbeiter) beigezogen wird.*

Die *Mitteilungspflicht* geht über die Regelung in der DSGVO hinaus und ist als Swiss Finish abzulehnen. Das Umsetzen dieser Mitteilungspflicht würde zu einem erheblichen Mehraufwand für die Firmen führen und gleichzeitig würden die Betroffenen in einer Flut von Meldungen untergehen.

Deshalb sollte der *Absatz gestrichen* werden.

- *Abs. 5: Informationspflicht gegenüber betroffener Person, wenn Daten bei einem Dritten beschafft werden*

Diese Regelung ist strenger als die Regelung in der DSGVO und verlangt, dass die betroffene Person spätestens bei der Speicherung der Daten informiert wird. In der Praxis werden Daten unmittelbar nach deren Beschaffung gespeichert und in den meisten Fällen erst nachher gelesen. *Eine Information der betroffenen Person bei der Speicherung ist praxisfremd* und kann nicht umgesetzt werden. Wir empfehlen hier eine *analoge Regelung, wie in der DSGVO*.

Art. 16 VE-DSG: Datenschutzfolgeabschätzung

Die Schweizerische Post nimmt bereits heute für jedes Projekt, welches Datenbearbeitungen umfasst, eine Einschätzung aus Datenschutzsicht vor. Die zwingende Benachrichtigung des EDÖB über die Ergebnisse der DS-Folgeabschätzung sowie der vorgesehenen Massnahmen erscheint jedoch nicht praktikabel. Auch macht es keinen Sinn, wenn der Auftragsdatenbearbeiter dieselben Pflichten in Bezug auf die Datenschutzfolgeabschätzung hat wie der Verantwortliche.

- *Abs.1: Neue Pflicht zur Durchführung einer Datenschutzfolgeabschätzung bei erhöhtem Risiko*

Die Regelung im VE-DSG zur zwingenden Datenschutzfolgeabschätzung bei *erhöhten Risiken* führt zu massivem zusätzlichen Mehraufwand mit entsprechenden Zusatzkosten und geht über die Vorgaben der EU-DSGVO hinaus. Eine solche Folgeabschätzung sollte deshalb nur bei einem hohen Risiko durchgeführt werden müssen, wobei das hohe Risiko seitens des Gesetzgebers konkretisiert werden muss.

- *Abs.3: Mitteilungspflicht an EDÖB*

Es wird zudem verlangt, dass der *EDÖB über die Ergebnisse informiert werden muss*. Die Schweizerische Post setzt eine grosse Menge an Projekten um. Wenn wir den EDÖB über jede durchgeführte Datenschutzfolgeabschätzung informieren müssten, wäre der EDÖB aufgrund der Anzahl von Meldungen gar nicht in der Lage, fristgerecht seinen gesetzlichen Verpflichtungen nachzukommen. Die Meldepflicht an den EDÖB sollte nur erfolgen, *wenn nach ergriffenen Massnahmen weiterhin ein erhöhtes Risiko besteht.*

Art. 17 VE-DSG: Meldung von Verletzungen des Datenschutzes

- *Abs.1: Neue, unverzügliche Meldepflicht an den EDÖB für jede unbefugte Datenbearbeitung*

Die Formulierung im Entwurf geht über die Regelung in der E-SEV 108 und der DSGVO hinaus, denn künftig muss jede Verletzung dem EDÖB gemeldet werden. Auf eine Meldung kann gemäss Entwurf nur verzichtet werden, wenn höchstwahrscheinlich keine Gefahr für die betroffene Person daraus resultiert, was jedoch in der Praxis kaum je der Fall sein dürfte, da jede unbefugte Datenbearbeitung eine Persönlichkeitsverletzung darstellt. Unter der Berücksichtigung, dass unsere Tochtergesellschaft PostFinance AG dem Bankkundengeheimnis untersteht, müsste PostFinance Verletzungen von Kundendaten melden und würde sich u.a. einer Strafverfolgung nach Art. 47 BankG aussetzen.

Die korrekte Umsetzung in der Praxis wäre auch mit enormem Zusatzaufwand realistischer Weise kaum möglich.

Die Pflicht zur Meldung von Verletzungen sollte so formuliert werden, dass diese nur erfolgen muss, wenn eine *grosse Menge von Personen betroffen ist oder die Verletzung qualitativ wesentlich* ist. Zudem sollte die Meldepflicht in *zeitlicher Hinsicht relativiert werden*, denn eine Meldung an den EDÖB macht nur Sinn, wenn wir ihn mit den relevanten Informationen dokumentieren können und dazu bedarf es vorgängig einiger Abklärungen. Zudem sollte insbesondere für die Finanzinstitute klargestellt werden, wie das Verhältnis respektive die Abgrenzung zur Meldepflicht gemäss Art. 29 Abs. 2 FINMAG ist.

Art. 19 VE-DSG: Weitere Pflichten

- *Abs. 1 lit. a: Neue Dokumentationspflicht*

Die Dokumentationspflicht der Datenbearbeitungen befürworten wir im Grundsatz. Die Ausgestaltung muss jedoch praktikabel sein und darf nicht zu viel administrativen Aufwand generieren. Eine Anlehnung an die Vorgaben in der DSGVO wäre wünschenswert.

Art. 50-51 VE-DSG: Strafbestimmungen

- *Art. 50 Abs. 4 und Art. 51 Abs. 2: Fahrlässigkeit*

Die Bestrafung fahrlässigen Verhaltens erscheint uns nicht sachgerecht und ist auch europarechtlich nicht erforderlich.
Die Strafbestimmungen fokussieren im Entwurf auf die flankierenden Massnahmen, d.h. primär werden Mitteilungs-, Informations-, oder Dokumentationspflichten sanktioniert. Eine fahrlässige Verletzung dieser Pflichten führt im Einzelfall wohl kaum zu einer gravierenden Verletzung der Persönlichkeit einer betroffenen Person. Zudem führt die fahrlässige Bestrafung zu einer Kriminalisierung aller Mitarbeitenden, da jeder Mitarbeiter bei jedem Entscheid, der sich als nicht richtig herausstellt, bereits gebüsst werden kann. *Die Begehung der Tatbestände durch Fahrlässigkeit ist daher zu streichen.*

Art. 53 VE-DSG: Übertretungen in Geschäftsbetrieben

Wir sind der Ansicht, dass die Sanktionen primär das Unternehmen und nicht unsere Mitarbeitenden treffen sollten. Gemäss aktuellem Entwurf, kann unter gewissen Voraussetzungen die Firma zur Bezahlung der Busse verurteilt werden. Die diesbezügliche Regelung im Vorentwurf geht in die richtige Richtung, sollte jedoch in jedem Fall anwendbar sein. Wir empfehlen die Klausel daher *nicht als „Kann – Vorschrift" auszuformulieren*. Zudem ist die festgelegte Grenze *von CHF 100'000 zu tief.*

Art. 59 VE-DSG: Übergangsbestimmungen

Der Gesetzesentwurf enthält viele Neuerungen, welche administrative und technische Anpassungen bedingen. Der Entwurf gewährt aktuell eine Übergangsfrist von zwei Jahren lediglich für die Einführung des Grundsatzes „Privacy by design" und „Privacy by default" bei bereits bestehenden Datenbearbeitungen sowie für die Datenschutzfolgeabschätzung. Die übrigen Pflichten müssten auf den Zeitpunkt des Inkrafttretens bereits umgesetzt sein. Dies erscheint uns unrealistisch. Wir schlagen daher vor, *eine generelle Übergangsfrist von zwei Jahren für alle Bestimmungen einzuführen.*

Wir bedanken uns für Ihre Kenntnisnahme und wohlwollende Prüfung der Eingabe.

Freundliche Grüsse

Post CH
Corporate Center

Markus Schumacher
Leiter Corporate Center

Gabriele Schmid
Datenschutzbeauftragte Konzern

Amstutz Jonas BJ

Von: Flueckiger Christian <christian.flueckiger@ppdt-june.ch>
Gesendet: Mittwoch, 8. März 2017 10:45
An: Amstutz Jonas BJ
Betreff: N/Réf: 2017.1722 Consultation révision LPD
Anlagen: Revision-totale-loi-PdD_Formulaire-FR_20170207.pdf

Cher Monsieur,

Vous trouverez en annexe la réponse à la consultation de la révision de la LPD.

Cordialement

Christian Flueckiger
Préposé à la protection des données
et à la transparence
Docteur en droit et avocat

PPDT - Préposé à la protection des données et à la transparence Jura Neuchâtel

Rue des Esserts 2
2345 Les Breuleux
T +41 32 420 90 92
F +41 32 420 90 91
www.ppdt-june.ch

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avis donné par

Nom / société / organisation : Préposé à la protection des données et à la transparence des cantons du Jura et de Neuchâtel

Abréviation de la société / de l'organisation : PPDT JU-NE

Adresse : Essert 2, 2345 Les Breuleux

Personne de référence : Christian Flueckiger, PPDT

Téléphone : 032.420.90.92

Courriel : Christian.flueckiger@ppdt-june.ch

Date : 08.03.2017

Remarques importantes :

1. Nous vous prions de ne pas modifier le formatage de ce formulaire !
2. Utilisez une ligne par article, alinéa et lettre ou par chapitre du rapport explicatif.
3. Veuillez faire parvenir votre avis au **format Word** d'ici au 4 avril 2017 à l'adresse suivante : jonas.amstutz@bj.admin.ch

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Nous vous remercions de votre collaboration!

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Table des matières

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Remarques générales

nom/société	remarque / suggestion :
	Au centre de la révision totale de la LPD on trouve la volonté de renforcer l'effet de la loi et des droits des personnes concernées. Dans ce cadre, la réforme s'oriente fortement aux développements qui interviennent au niveau européen. En matière de renforcement des droits des personnes concernées, l'AP ignore toutefois des éléments centraux de la réforme dans l'UE: l'art. 20 règlement (UE) 2016/679 prévoit un droit à la portabilité de la personne concernée (recevoir les données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine). En outre, l'art. 17 règlement (UE) 2016/679 régit le droit à l'oubli. Ces deux droits renforcent la position de la personne concernée à l'égard des grands acteurs globaux qui traitent des données. On ne voit pas pourquoi les citoyennes et les citoyens suisses devraient être privés de ces droits. Dès lors, nous proposons une analyse sérieuse relative à l'insertion de ces deux instruments juridiques dans la révision totale de la LPD.

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

nom/société	loi	art.	al.	let.	remarque / suggestion :
	LPD	1			D'accord avec le fait de ne plus protéger que les personnes physiques
	LPD	2	2	c	L'exclusion de la jurisprudence ne correspond pas à la convention STE 108 qui ne prévoit pas de

					possibilité d'introduire d'exception au champ d'application. Nous proposons de prévoir la réglementation suivante: Les principes généraux de la LPD (c.-à-d. p.ex. les principes concernant la sécurité informatique, la consultation préalable etc.) s'appliquent aussi aux instances judiciaires. Les codes de procédure sont, quant à eux, considérés comme droit de la protection des données sectorielle (c.-à-d. lex specialis; voir Beat Rudin, Überholte Ausnahme im Geltungsbereich, digma 2016, p. 122 ss). Seules deux exceptions au champ d'application sont nécessaires et conformes avec la convention STE 108 (comme proposé, par ailleurs, par la Conférence des gouvernements cantonaux dans son guide pratique relatif à la mise en oeuvre dans les LPD cantonales): • Afin d'éviter la collision des droits de la personne concernée avec les droits de procédure des parties au procès: il peut être prévu (à l'art. 2 AP-LPD) que durant une procédure en cours les droits et prétentions de la personne concernée sont exclusivement régis par le droit de procédure applicable. Ainsi, durant le procès, les parties ne peuvent faire valoir que leur droit d'accès lié à la procédure en cours et ne peuvent se fonder sur le droit d'accès relatif à la protection des données (accès à leurs données personnelles). • Afin d'éviter la collision des droits et obligations de surveillance: il peut être prévu (p.ex. à l'art. 40 AP-LPD) que le traitement de données dans des procédures judiciaires en cours auprès d'instances fédérales échappent à la surveillance du PFPDT.
	LPD	2	3		Voir remarques relatives à l'art. 2 al. 2 lit. c AP-LPD En outre: est-ce que les tribunaux (en dehors de leur activité contentieuse) sont exclus de manière générale de la surveillance par le PFPDT ou est-ce qu'il ne peut simplement pas prendre des ordonnances à leur encontre (comme proposé par la Conférence des gouvernements cantonaux dans son guide pratique relatif à la mise en oeuvre dans les LPD cantonales)?
	LPD	3		a	Ch. 2: nous approuvons la prise en compte du critère «ethnie» (appartenance à un groupe d'êtres humains qui se sentent liés entre eux sur le plan culturel, historique, linguistique, des moeurs, des traditions et des coutumes et qui vivent donc dans une communauté ressentie comme différente du

					reste de la population et/ou qui sont perçus comme tels par le reste de la population) En revanche, nous proposons de supprimer le terme de «race». Ce terme n'a pas de portée scientifique pour l'être humain. Ce que l'on veut protéger, c'est plutôt le reproche de l'appartenance à une race (sur le plan historique: les «juif», les «nègre» etc).
	LPD	3		c	Ch. 3: nous approuvons la prise en compte des «données génétiques» dans le catalogue des données sensibles.
	LPD	3		c	Ch. 4: Le terme de «données biométriques» est équivoque. Le rapport explicatif ne clarifie pas la question. Or, l'image d'un visage (un portrait) constitue, en principe, aussi une donnée biométrique, mais il ne s'agit pas de la soumettre, comme sous-catégorie, à la protection des données sensibles. Ainsi, comme le fait la Conférence des gouvernements cantonaux dans son guide pratique relatif à la mise en oeuvre dans les LPD cantonales, nous proposons de reprendre la définition suivante: «4. des données à caractère personnel résultant d'un traitement technique spécifique relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique (données biométriques)».
	LPD	3		d	Le terme «enregistrement» contredit la principe de la formulation neutre de la loi (sur le plan technologique, de la loi).
	LPD	3		d	Dans l'avant-projet (art. 4 al. 5, art. 25 al. 1, art. 29 et 30) ainsi que dans la directive [UE] 2016/680), les notions «effacer» et «détruire» sont utilisées côte à côte, sans que le rapport entre les deux soit tiré au clair. Par la destruction, à ce jour, on entendait la destruction physique. Il faut encore déterminer, si l'effacement vise uniquement l'élimination du processus actif (comme, p.ex., effacer des inscriptions du casier judiciaire) ou la destruction dans le contexte électronique. Nous proposons donc de clarifier la question dans la loi ou, du moins, dans le texte du message du Conseil fédéral.
	LPD	3		f	Nous approuvons le remplacement du notion peu claire de «profil de la personnalité» par la notion de «profilage» (comme type «dangereux» de traitement de données personnelles). Toutefois, il serait

					absolument insuffisant que, dans le droit de protection des données sectoriel (donc dans les lois fédérales que l'on doit adapter), le profilage soit introduit sans aucune retenue par des normes constituant de véritables blancs-seings. Un cadre législatif clair et restrictif est requis pour concretiser le profilage dans la législation fédérale.
	LPD	3		i	Nous proposons de parler, en droit suisse, de «sous-traitant en matière de traitement de données». En effet, cette personne n'est pas simplement chargée d'un mandat quelconque. Elle doit traiter des données personnelles pour le compte du responsable du traitement. Il n'est pas problématique de s'écarter de la terminologie européenne, dès lors que c'est déjà le cas pour d'autres notions (p.ex. en allemand on parle à juste titre de «Bearbeiter» et non de «Verarbeiter» dans ce contexte). L'intitulé de l'art. 7 AP-LPD (sous-traitance) doit logiquement être complété (sous-traitance en matière de traitement des données), comme c'est déjà le cas dans la version allemande du texte.
	LPD	3			Nous approuvons l'abandon de la notion de «fichier». A l'ère digitale, cette terminologie est totalement surannée et ne correspond à plus rien dans le contexte informatique.
	LPD	4	4		Nous approuvons la nouvelle formulation et les adjonctions opérées à l'art. 4 AP-LPD. Il convient de relever que l'art. 4 al. 4 AP-LPD implique la détermination de durées de conservation. Cette obligation du responsable du traitement devrait au moins être évoquée dans le texte du message du Conseil fédéral.
	LPD	4	6		Nous approuvons le fait que selon l'art. 4 al. 6 AP-LPD le consentement ne doive pas seulement être donné librement, mais aussi clairement. La deuxième phrase indique que le consentement doit, dans certaines conditions, être «exprès». Cette notion a été discutée de manière controversée dans la doctrine. Il convient donc d'en clarifier le contenu, au moins dans le texte du message du Conseil fédéral.
	LPD	7			Cette disposition reprend largement la formulation de l'actuel art. 10a LPD. De ce fait, les exigences européennes (en particulier des art. 22 sv. de la directive [UE] 2016/680) ne sont pas formulées correctement les organes fédéraux.

					Pour ce qui est de la notion utilisée dans l'intitulé, il convient d'adapter la terminologie, comme cela a été indiqué pour l'art. 3 lit. i AP-LPD (sous-traitance en matière de traitement de données).
	LPD	7	1	a	Le responsable du traitement des données personnelles ne doit pas seulement s'assurer du respect de la sécurité des données et des droits des personnes concernées, mais il doit garantir ce respect par des mesures efficaces, de telle sorte que les données ne soient traitées que de la manière qu'il serait en droit de faire lui-même. La formulation de l'art. 7 al. 1 lit. a AP-LPD doit donc être complétée.
	LPD	7	2		L'art. 7 al. 2 AP-LPD doit être reformulé selon ce qui vient d'être indiqué pour l'art. 7 al. 1 lit. a AP-LPD. En outre, il ne suffit pas de préciser les exigences à l'égard des sous-traitants en matière de traitement de données. Il faut aussi concrétiser les obligations du responsable du traitement des données personnelles, notamment dans le choix du sous-traitant et dans les mesures à prendre pour garantir le traitement des données dans le cadre de ce que le responsable serait en mesure de faire lui-même. Une telle concrétisation doit intervenir au niveau de l'ordonnance.
	LPD	8			Le nouvel instrument de la recommandation des bonnes pratiques, édictées ou approuvées par le PFPDT, prète flanc à la critique. Cet instrument est vorace de ressources, s'il doit aboutir à des recommandations, efficaces dans la pratique et qui interviennent à temps, après la consultation des milieux intéressés et compte tenu des particularités des domaines concernés. Tant que l'on n'a pas démontré comment ces ressources sont mises à dispositon du PFPDT, cet instrument doit être considéré comme inefficace.
	LPD	9	1+2		Le libellé de l'art. 9 AP-LPD n'exprime pas de façon assez claire le fait que le respect des recommandations de bonnes pratique constitue uniquement une présomption légale du respect du droit de la protection des données. En règle générale, les recommandations de bonnes pratiques constituent une concrétisation de la loi. Toutefois, elles ne parviennent jamais à concrétiser la loi dans son ensemble. Ainsi, leur respect ne constitue qu'un aspect parmi plusieurs pour juger si un traitement de données respecte la loi. Cette conclusion est soulignée par le fait que le respect des recommandations de bonnes pratiques est facultative (al. 2). De ce fait, on pourrait supprimer l'art. 9 AP-LPD, sans qu'une telle suppression ne produise un effet sur la portée de la loi.

	LPD	10			Le rapport explicatif relatif à l'art. 10 AP-LPD prétend qu'il n'y a pas de différence avec l'actuel art. 11 LPD. Toutefois, l'art. 10 AP-LPD ne parle plus que des «opérations de traitement» alors que l'art. 11 LPD évoque explicitement les «systèmes de logiciels et de traitement de données». La modification du libellé de la disposition n'est donc pas indiquée dans le rapport explicatif qui admet que les systèmes de logiciels et de traitement de données sont aussi visés par la loi. Par ailleurs, la certification est réservée au responsable du traitement des données ou au sous-traitant (en matière de traitement des données), ce qui, justement, exclut la certification de produits. Dès lors que la certification des produits est restée lettre morte selon le droit actuel, il est sans autre admissible de la supprimer. Mais, dans ce cas, il faut l'indiquer clairement dans le texte du message du Conseil fédéral.
	LPD	11			L'art. 11 AP-LPD reprend l'actuel art. 7 LPD. Toutefois, il omet de définir des objectifs de protection comme le font l'art. 32 al. 1 lit. b règlement (UE) 2016/679 et l'art. 29 al. 2 directive (UE) 2016/680. De tels objectifs sont, par ailleurs, aussi édictés par certaines lois cantonales plus récentes sur la protection des données (voir p.ex. § 7 IDG/ZH ou § 8 IDG/BS). Dans ce contexte, il faut aussi revoir la terminologie du «traitement non autorisé». Enfin, le libellé en langue française de la norme est plus correct que celui en langue allemande, dans la mesure où il oblige de prendre des mesures «contre tout traitement non autorisé et toute perte» (en allemand, le «et» est remplacé par un «ou). En définitive, nous proposons d'évoquer de façon explicite les objectifs de protection dans le texte de la loi.
	LPD	12			Sur le principe, nous approuvons l'introduction d'une norme régissant l'accès aux données d'une personne décédée. Toutefois, nous doutons que la disposition prévue puisse répondre aux exigences d'une telle situation. Une interdiction au sens de l'art. 12 al. 1 lit. a AP-LPD n'interviendra que très rarement en pratique. Donc, conformément à l'art. 12 al. 1 lit. b AP-LPD, dans la majorité des cas, la décision découlera d'une pondération des intérêts. Or, pour le responsable du traitement des données personnelles, la prise en compte des intérêts de la personne défunte n'est pas aisée et il ne parviendra pas sans autre à déterminer ou à pondérer ces intérêts (si on ne part pas de l'idée qu'au moment du décès les intérêts de la personne défunte «s'éteignent» automatiquement). Ainsi, nous proposons de vérifier si la

					disposition ne doit pas être formulée de manière plus restrictive.
	LPD	12	3		Nous considérons que la mise en échec des secrets de fonction (surtout ceux qui dépassent le cadre du droit du travail) et des secrets professionnels, simplement sur la base de la pondération des intérêts (art. 12 al. 1 AP-LPD) est problématique. Seules les autorités de surveillance compétentes doivent pouvoir délier le professionnel du secret qu'il doit préserver. Nous proposons de supprimer cette disposition ou de la formuler de manière plus restrictive.
	LPD	15			La portée de cette disposition se vérifie surtout dans le contexte du droit privé. Pour ce domaine, nous approuvons son contenu. Pour ce qui est du droit public, les actes individuels produisant un effet juridique sont, en règle générale, pris en la forme de décisions. Ces décisions doivent être notifiées, en garantissant, par ce biais, l'information des personnes concernées. Par ailleurs, le droit d'être entendu des personnes concernées leur permet de s'exprimer avant la notification de la décision en question. Pour ce motif, la Conférence des gouvernements cantonaux affirme, dans son guide pratique relatif à la mise en oeuvre dans les LPD cantonales, qu'aucune réglementation n'est nécessaire dans les lois cantonales (sur l'information et) sur la protection des données. Dès lors et sous réserve de l'alinéa 3, nous proposons de placer cette disposition dans la section de la loi réservée au traitement de données personnelles par des personnes privées. Pour ce qui est du domaine du droit public, nous proposons de n'admettre des actes individuels automatisés des autorités dans une autre forme que la décision qu'aux conditions suivantes: • une loi formelle le prévoit expressément; • simultanément la loi indique les mesures à prendre afin de garantir les droits de la personne concernée (en particulier pour ce qui est de la transparence et des possibilités d'intervention de la personne concernée).
	LPD	16			Nous proposons de règler les questions de l'analyse d'impact relative à la protection des données (art. 16 al. 1 et 2 AP-LPD) et de la consultation préalable du préposé (art. 16 al. 3 et 4 AP-LPD) dans deux

					dispositions distinctes. Comme mesure la plus efficace de la protection des données préventive (au moins pour le traitement des données par des organes fédéraux), la consultation préalable doit être déclarée obligatoire lorsque le traitement des données conduit à un risque accru pour la personnalité ou pour les droits fondamentaux de la personne concernée.
	LPD	16	1+2		L'analyse d'impact relative à la protection des données doit intervenir dans tout projet de traitement des données. La condition forumlée au premier alinéa (lorsque le traitement envisagé est susceptible d'entraîner un risque accru pour la personnalité et les droits fondamentaux) est déjà le résultat d'un premier pas de l'analyse d'impact. En vérité, l'analyse d'impact relative à la protection des données n'est rien d'autre que la préparation du responsable du traitement des données qui le conduit à pouvoir documenter le respect des dispositions de la protection des données au sens de l'art. 19 lit. a AP-LPD. Par ailleurs, l'analyse d'impact concerne les mêmes points qui doivent être élaborés en vue d'une consultation préalable, lorsqu'un projet conduit à un risque accru pour la personnalité et pour les droits fondamentaux (art. 16 al. 3 et 4 AP-LPD).
	LPD	16	3+4		La consultation préalable, telle que prévue à l'art. 8bis de la convention STE 108 et à l'art. 28 de la directive (UE) 2016/680, n'est pas mise en oeuvre de manière suffisante aux art. 16 al. 3 et 4 AP-LPD. La consultation préalable (ou le contrôle préalable, tel que, dans les textes européens, on dénommait par le passé l'instrument en question) aurait déjà dû être introduite avec la convention Schengen-Dublin. Comme le montre la pratique bien établie dans les cantons, il s'agit là de l'un des moyens les plus efficaces de la protection des données préventive. Dès lors, nous proposons qu'aux conditions suivantes les résultats de l'analyse d'impact relative à la protection des données ainsi que les mesures de protection doivent impérativement être soumis à la consultation préalable du préposé: un risque accru* pour la personnallité (dans le cadre du traitement des données par des privés) ou pour les droits fondamentaux (pour les traitements de données par des organes fédéraux soumis au droit public) sont établis. Le préposé doit alors vérifier si les risques pour les droits fondamentaux des personnes concernées ont été suffisamment pris en compte ou préservés par les mesures proposées par le responsable du traitement des données. * L'art. 28 de la directive (UE) 2016/680 parle d'un «risque élevé». Dans la terminologie, cela

					correspond au concept de protection des droits fondamentaux de l'office féréral allemand de sécurité informatique (BSI), très répandu en Suisse allemande. Pour le BSI, un «risque plus élevé» existe p.ex. lorsque des données sensibles sont traitées. Un tel traitement exige, en plus de la protection usuelle, la prise de mesures de protection particulières. En revanche, un «risque élevé» exigerait des mesures de protection de haute sécurité, ce qui ne devrait concerner qu'un nombre très restreint d'applications.
	LPD	17	1		L'art. 17 al. 1 AP-LPD ne définit pas clairement les «violations de la protection des données». Au vu d'une possible sanction pénale du responsable du traitement des données (voir art. 50 al. 2 lit. e et art. 50 al. 3 lit. b AP-LPD), une telle définition s'avère indispensable (voir aussi nos remarques relatives aux art. 50 ss AP-LPD). La définition doit être indiquée dans cette disposition ou alors à l'art. 3 AP-LPD (définitions légales). Confromément au guide pratique de la Conférence des gouvernements cantonaux relatif à la mise en oeuvre dans les LPD cantonales, nous proposons la notion suivante: «Il y a violation de la protection des données dès lors que l'atteinte à la sécurité est telle qu'elle a entraîné la suppression définitive ou la perte des données traitées, leur modification ou leur divulgation non intentionnelle ou illicite, ou que des personnes non autorisées ont accès à ces données personnelles.» L'obligation de notifier doit, selon l'AP, ne pas s'appliquer lorsque la violation ne présente vraisemblablement pas de risques pour la personnalité et les droits fondamentaux de la personne concernée. Cette formulation laisse un large pouvoir d'appréciation au responseble du traitement des données qui, de fait, exclut la punissabilité pour une omission intentionnelle ou par négligence. Le pouvoir d'appréciation doit, dès lors, être restreint de façon plus concrète et il convient de revoir l'application du droit pénal en la matière (voir aussi nos remarques relatives aux art. 50 ss AP-LPD).
	LPD	18	1		Le libellé de l'art. 18 al. 1 AP-LPD n'indique pas clairement, dans quelle mesure la dispostion impose une obligation supplémentaire par rapport à l'art. 11 AP-LPD. C'est pourquoi la possible sanction pénale pour l'omission de prendre des mesures (art. 51 al. 1 lit. e AP-LPD) semble discutable. En accord avec l'art. 11 AP-LPD, la protection des données par le biais de la technologie est l'une des mesures possibles. C'est pourquoi il faut relier l'art. 18 al. 1 AP-LPD à l'art. 11 AP-LPD.
	LPD	18	2		Comme l'insinue le rapport explicatif, l'art. 18 al. 2 AP-LPD n'a de portée que dans le contexte du droit

					privé, dès lors que les organes fédéraux ne peuvent traiter des données qu'au moyen d'une base légale (art. 27 AP-LPD). Dès lors, il convient d'adapter le libellé. Par ailleurs, il serait aussi possible de placer l'al. 2 dans le cadre de l'art. 4 AP-LPD.
	LPD	19	1		Contrairement à ce qu'affirme le rapport explicatif, il convient de préciser que l'obligation de documenter les traitements de données personnelles, telle qu prévue au lit. a ne répond ni aux exigences de l'art. 8bis ch. 1 du projet de la convention STE 108 ni à celles de l'art. 4 al. 4 directive (UE) 2016/680. Le responsable du traitement des données personnelles et le sous-traitant (en matière de traitement de données personnelles) doivent pouvoir *prouver* qu'ils respectent les dispositions de protection des données. Cette exigence dépasse le cadre d'un registre du traitement des données personnelles. Un telle preuve peut être apportée à l'aide d'un véritable système de gestion de la protection des données (Datenschutzmanagementsystem ou DSMS en allemand). Un tel DSMS doit répondre aux standards de qualité de gestion et de sécurité informatique édictés par les normes ISO (ISO 9001 et ISO 27001 etc.). Si l'on renonce à un tel certificat de qualité, il faut déterminer les documents nécessaires pour pouvoir apporter la preuve requise (concept de sécurité informatique, concept d'accès aux données etc.). Il existe déjà de nombreuses publications en la matière. Il serait pertinent de déterminer, dans l'ordonnance, les cas dans lesquels un DSMS est tenu pour obligatoire (p.ex. en cas de traitement de données sensibles). Par ailleurs, une réglementation très claire est nécessaire, dès lors que l'omission de documenter peut entraîner une sanction pénale (art. 51 al. 1 lit. f. AP-LPD; voir aussi nos remarques relatives aux art. 50 ss AP-LPD). Une telle sanction n'est licite que dans la mesure où le contenu de la norme légale est suffisamment déterminé.
	LPD	20	1		Nous approuvons la gratuité postulée pour l'exercice du droit d'accès (aux données personnelles de la personne concernée). En effet, le droit d'accès constitue la clé de voûte de l'autodétermination informationnelle.

	LPD	20	2		Nous approuvons l'énumératon expresse, dans la loi, des informations qui doivent être communiquées à la personne concernée.
	LPD	23	2	d	Pour le profilage, il n'est pas utile de prévoir, dans la disposition, le consentement comme fait justificatif excluant la tyicité. Dans le sens de la notion légale (voir ci-dessus notre proposition de complément à l'art. 3 lit. f AP-LPD), le profilage constitue une atteinte à la personnalité. Cette atteinte peut, comme prévu à l'art. 24 al. 1 AP-LPD, être justifiée par le consentement de la personne concernée. De application de l'art. 4 al. 6 AP-LPD il ressort clairement que ce consentement doit être exprès. Dès lors, nous proposons de tracer le passage suivant de la disposition: «sans le consentement exprès de la personne concernée».
	LPD	24	2	c	Ch. premier: selon le droit en vigueur, les traitements de données par des entreprises d'analyse de solvabilité sont couvert par un intérêt prépondérant, tant qu'il n'y a pas constitution de profil de la personnalité. L'AP-LPD remplace de terme de profil de la personnalité (comme type de donnés «dangereuses») par le profilage (comme type de traitement des données «dangereux»). A l'art 24 al. 2 lit. c AP-LPD on permet le profilage sans que – à l'exception de la majorité de la personne concernée (ch. 3) – il n'y ait d'exigences plus sévères imposées à ce profilage. Nous proposons de vérifier ce problème et d'imposer des exigences plus sévères au profilage pour l'analyse de la solvabilité.
	LPD	25			Très souvent il est pratiquement exclu, pour les personnes concernées, d'apporter la preuve du traitement de leurs données par des entreprises avancées dans l'utilisaiton de l'informatique. Ainsi les actions de l'art. 25 AP-LPD (aujourd'hui l'art. 15 LPD) manquent d'efficacité. Aussi, nous proposons d'introduire un renversement du fardeau de la preuve pour les actions de l'art. 25 AP-LPD, afin de renforcer la position de la personne concernée en cas de conflit.
	LPD	25			Voir notre proposition relative à l'art. 3 lit. d AP-LPD (effacer – détruire)
	LPD	26	1		Le rapport entre l'art. 3 lit. h et l'art. 26 AP-LPD n'est pas clair. Selon l'art. 3 lit. h AP-LPD l'organe

					fédéral qui l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités, les moyens et l'étendue du traitement de données personnelles en assume la responsabilité. Selon l'art. 26 al. 1 AP-LPD, il incombe à l'organe fédéral responsable de pourvoir à la protection des données personnelles qu'il traite ou fait traiter. La relation entre ces deux dispositions doit être tirée au clair.
	LPD	27	1		Nous déduisons de l'art. 27 al. 1 AP-LPD qu'à l'avenir les deux formes de bases légales suivantes semblent suffir pour le traitement de données personnelles «ordinaires»: • des bases légales directes, dans lesquelles le traitement des données est régie de façon expresse, et • des bases légales indirectes, dans lesquelles une tâche est imposée à un organe fédéral, dont la mise en oeuvre suppose impérativement le traitement de données personnelles («ordinaires»). En d'autres termes, un organe fédéral peut traiter des données personnelles (mais uniquement «ordinaires») lorsque cela est exigé par une activité imposée par la loi (pour le traitement de données sensibles, les exigences plus restrictives de l'al. 2 s'appliquent: la tâche doit être clairement prévue dans une loi au sens formel et le traitement de données n'est licite que s'il est indispensable à l'accomplissement de la tâche ou comme le prévoient certaines lois cantonales: le traitement de données doit être impérativement nécessaire). Nous proposons de tirer au clair la question soit dans la loi, soit au minimum dans le message du Conseil fédéral.
	LPD	27	2		Nous revenons à notre remarque préliminaire relative au profilage (voir remarque relative à l'art. 3 lit. f AP-LPD): des garanties suffisantes doivent être prévues dans la loi afin de protéger les droits fondamentaux des personnes concernées. Des blancs-seings (p.ex. «l'office fédéral est autorisé à traiter des données sensibles et à procéder à un profilage») ne peuvent en aucun cas être introduits dans la législation. Par conséquent, nous proposons d'ancrer le profilage de manière impérative dans une loi au sens formel (en effet, le profilage est toujours source de risques particuliers pour la personnalité et pour les droits fondamentaux des personnes concernées; donc, conformément à l'art. 27 al. 2 lit. b AP-LPD il

					ne peut se satisfaire d'une base légale matérielle). Afin d'expliciter plus clairement notre idée, nous proposons de formuler l'art. 27 al. 2 AP-LPD de la manière suivante: Une loi au sens matériel suffit pour le traitement de données personnelles sensibles, si …
	LPD	27	2	b	Nous proposons de supprimer la notion de «personnalité». Les risques pour la personnalité sont surtout le fait du traitement des données par des personnes privées. Lorsque le traitement des données émane d'organes fédéraux, on parle de risques pour les droits fondamentaux. Dès lors que cette disposition régit exclusivement le traitement de données personnelles par des organes fédéraux, il convient de supprimer la notion de «personnalité».
	LPD	31	2		Voir notre proposition relative à l'art. 3 lit. d AP-LPD (effacer – détruire). Si dans cette disposition on veut vraiment régir exclusivement le destruction (selon la notion expliquée), la formulation est correcte. Sinon, on doit vérifier s'il ne faudrait pas plutôt formuler comme suit: Ils effacent ou détruisent...
	LPD	34	1	a	Nous proposons une modification de la version allemande de l'AP: a. die widerrechtliche Bearbeitung von Personendaten unterlässt (suppression du mot «betreffenden»).
	LPD	34	4		Voir notre proposition relative à l'art. 3 lit. d AP-LPD (effacer – détruire).
	LPD	36			Une des nouveautés consiste à obliger les organes fédéraux responsables à déclarer leurs activités de traitement de données personnelles. Selon le rapport explicatif (p. 71 sv.), cette obligation consisterait principalement à annoncer certains fichiers. Il s'agirait donc surtout d'une adaptation de la terminologie puisque la révision supprime la notion de «fichier» (art. 3 litt. g LPD). Cette explication méconnait le fait qu'il ne s'agit justement pas simplement de remplacer la notion de «fichier». Il faut bien plutôt questionner de manière critique l'apport, à ce jour, du registre des fichiers à la protection des droits fondamentaux des personnes concernées. Nous proposons de réduire le fichier aux *activités de traitement de données* en reprenant ce que certains cantons ont pu faire (voir p.ex. § 24 IDG/BS qui exige une liste des procédures conduisant à traiter des données personnelles; http://www.staatskanzlei.bs.ch/oeffentlichkeitsprinzip/verfahren.html).

	LPD	37			L'art. 37 AP-LPD régit la nomination et le statut du PFPDT. La terminologie du projet en français reprend la terminologie existante, alors que ce n'est pas le cas en allemand (la notion de «Wahl» étant remplacée par celle de «Ernennung»). Cette adaptation, en allemand, à la terminologie européenne est troublante, car elle ne correspond pas à la procédure: le titre, en allemand, doit être adapté au texte de l'al. 1 qui contient la notion correcte.
	LPD	37	4		La compétence budgétaire du PFPDT doit être aménagée de manière analogue à celle du contrôle des finances (CdF), selon la loi fédérale sur le Contrôle fédéral des finances (LCF, RS 614.0). Le PFPDT jouit de la même indépendance que le CdF. Cette indépendance doit aussi être réalisée sur le plan financier. Cela inclut la possibilité de soumettre directement sa proposition de budget au parlement, sans intervention du Conseil fédéral. Donc, comme c'est prévu à l'art. 2 al. 3 LCF, le préposé remet son projet de budget annuel au Conseil fédéral. Celui-ci le transmet, sans le modifier, à l'Assemblée fédérale.
	LPD	38	1		Il n'y a pas à restreindre la possibilité der renouveler le mandat du préposé. On ne comprend pas en quoi l'indépendance du préposé serait affaiblie si son mandat durait plus de 12 ans. Ni la directive (UE) 2016/680 ni le projet convention STE 108 ne comportent une telle durée maximale du mandat du préposé. La directive ne s'exprime que sur le fait qu'il convient d'ancrer dans la loi si et combien de fois le mandat du ou des membres d'une autorité de surveillance peut être reconduit.
	LPD	39	1		Il est inutile d'interdire au préposé d'exercer une fonction dans *un canton*. En matière de protection des données, le préposé ne peut ni donner des directives ni exercer de surveillance à l'égard des cantons et on ne voit pas en quoi une activité, par exemple bénévole, au niveau cantonal ou communal pourrait remettre en cause son indépendance.
	LPD	41			Nous approuvons la volonté d'étendre les moyens d'enquête du préposé. Cela répond aux exigences de l'art. 12bis ch. 3 projet convention STE 108 et de l'art. 52 directive (UE) 2016/680. Toutefois, ces dispositions indiquent clairement que le préposé n'est pas libre dans la décision de savoir s'il se saisit ou non d'un dossier suite à la plainte de la personne concernée. Dans un tel cas, il est évident qu'il est

					tenu d'instruire. Cette obligation doit être indiquée de manière plus claire à l'art. 41 al. 5 AP-LPD. Dès lors, il faut aussi lui attribuer bien plus de ressources, pour cette extension des moyens d'enquête, que ce qui est prévu au rapport explicatif, à savoir un ou deux postes. Il est pertinent de ne faire la planification des ressources que dans le message du Conseil fédéral. Mais, il est d'emblée clair qu'un ou deux postes ne suffiront en aucun cas.
	LPD	41	5		Le libellé de l'art. 41 al. 5 AP-LPD n'est pas suffisamment déterminé. Bien qu'il ne faille pas partir de l'idée que le préposé a un devoir d'enquête à proprement parler, il faut tout-de-même postuler qu'il soit *obligé de se saisir* du dossier. Selon les art. 52 sv. directives (UE) 2016/680 l'art. 41 AP-LPD vise une «réclamation auprès d'une autorité de contrôle». Dès lors, le préposé est obligé d'entrer en matière. L'art. 41 al. 5 AP-LPD doit être reformulé en fonction de cette obligation. En outre, la disposition devrait fixer un délai de traitement de trois mois. Dans tous le cas, il appartient au moins au message du Conseil fédéral de clarifier cette situation. Pour ce qui est de la question des ressources, voir les remarques relatives à l'art. 41 AP-LPD.
	LPD	43			En vertu de l'art. 43 AP-LPD, le préposé ne pourrait prendre que des mesures administratives, s'il constate que des dispositions de protection des données ont été violées. En application du droit européen il doit, au contraire, disposer de possibilités de sanctions efficaces et dissuasives (art. 12bis al. 2 lit. c projet convention STE 108). Selon le rapport explicatif, l'objectif visé doit être atteint sans possibilités de sanctions de la part du préposé et donc, exclusivement à l'aide de l'élargissement de l'appareil de sanctions pénales, introduit aux art. 50 ss AP-LPD. Toutefois, un tel élargissement des normes pénales n'apparaît pas comme une mesure adéquate pour assurer la mise en oeuvre de la protection des données (voir aussi nos remarques relatives aux art. 50 ss AP-LPD). Pour cette raison, le préposé doit avoir la possibilité d'imposer des véritables sanctions administratives (dont l'amende) et ce au moins à l'encontre des personnes privées. L'art. 43 AP-LPD doit donc être complété dans ce sens.
	LPD	45			En plus de l'*obligation* de dénoncer, il convient d'introduire, à l'art. 45 AP-LPD, un *droit* de dénoncer. Ce droit du préposé découle de l'art. 301 du code de procédure pénale (CPP; RS 312.0) et se rapporte aussi à des infractions qui ne seraient pas poursuivies d'office.

	LPD	49		a	Le préposé ne dispose pas de pouvoirs de surveillance ou de conseil à l'encontre des organes cantonaux (voir aussi nos remarques relatives à l'art. 39 al. 1 AP-LPD). Dès lors, il convient de maintenir, pour les relations avec les organes cantonaux, la formulation actuelle de l'art. 31 lit. a LPD (assister les organes … cantonaux).
	LPD	50			Remarque préliminaire relative aux art. 50-55 AP-LPD: Nous rejetons l'idée d'élargir les normes pénales dans l'AP-LPD. Avec l'introduction de nouvelles sanctions pénales, on semble mettre le déficit dans la mise en oeuvre de la protection des données sur le dos du droit pénal. On ignore par là que les dispositions pénales actuelles n'ont pas démontré leur efficacité dans une mise en oeuvre unitaire du droit de la protection des données. Il n'y a quasiment pas eu de sanctions pénales liées aux dispositions pénales actuelles de la LPD. Avec les nouvelles dispositions, le juge pénal entre en concurrence avec l'autorité de surveillance de la protection des données. Cela n'est pertinent ni sur le plan institutionnel ni sur le plan pratique. Un nombre important des nouvelles dispositions pénales ne répond pas à l'exigence d'un contenu suffisamment déterminé et violent, par là, le principe «nulla poenae sine lege» (voir aussi nos remarques relatives aux art. 50 et 51 AP-LPD). Par ailleurs, les dispositions pénales prévues ne répondent pas non plus complètement aux exigences de la directive (UE) 2016/680 et de l'art. 12bis al. 2 lit. c projet STE 108). Aussi bien l'UE que le Conseil de l'Europe exigent explicitement d'accorder le pouvoir, au préposé, de prendre des sanctions administratives (voir aussi nos remarques relatives à l'art. 45 AP-LPD). La possibilité d'infliger une amende maximale de CHF 500'000.- n'est absolument pas dissuasive pour des entreprises actives dans un marché global et bien en-deçà des possibilités de sanction prévues dans le droit européen. En outre, les dispositions pénales délèguent la poursuite pénale aux cantons. De ce fait, les cantons devraient augmenter leurs ressources pour la mise en oeuvre de l'AP-LPD. De plus, au vu de la

					matière particulière que représente la protection des données, on doit craindre une application non unitaire des dispositions pénales, si l'on se fonde sur une juridiction cantonale. La mise en oeuvre de l'AP-LPD et donc la poursuite pénale y relative sont, de notre point de vue, affaire de la Confédération et celle-ci doit donc l'assumer (voir aussi nos remarques relatives à l'art. 54 AP-LPD). Il en découle que le pouvoir de sanction du préposé doit être étendu (voir aussi nos remarques relatives à l'art. 43 AP-LPD) et que son organisation doit être étoffée de manière analogue à celle de la commission de concurrence (voir rapport explicatif, p. 78). En définitive, la compétence de sanctionner doit être attibuée au préposé et la loi doit être reformulée en conséquence.
	LPD	50			Nous constatons que l'amende maximale se monte à CHF 500'000.- respectivement à CHF 250'000.- en cas de négligence. De tels montants ne produisent pas un effet dissuasif, raison pour laquelle il faut les augmenter. Pour comparaison: dans l'UE une amende peut aller jusqu'à 20'000'000 Euro resp., pour des entreprises, jusqu'à 4 % du chiffre d'affaires réalisé sur le marché mondial au cours de l'exercice comptable écoulé; le montant le plus élevé sera retenu (voir art. 83 al. 5 règlement [UE] 2016/679). Voir aussi nos remarques relatives à l'art. 53 AP-LPD concernant les contraventions au sein des entreprises.
	LPD	50	1,2,3		Le contenu de la norme n'est pas suffisamment déterminé, raison pour laquelle la punissabilité n'est pas assurée. Citons, comme exemple, le devoir d'informer la personne concernée selon l'art. 15 AP-LPD: celui-ci existe lorsqu'une décision «affecte de manière significative» une personne. Comme élément objectif de la typicité, il est peu vraisemblable que «l'affection significative» soit assez précis pour répondre aux critères de la réserve d'une base légale au sens du droit pénal.
	LPD	51			Comme constaté dans le contexte de l'art. 50, cette norme n'est pas non plus assez déterminée.
	LPD	52			L'art. 52 vise à compléter la protection contre la violation du secret professionnel, telle que prévue à l'art. 321 du Code pénal Suisse (CPS; RS 311.0; voir aussi rapport explicatif, p. 81). Toutefois, cet objectif ne peut être atteint à l'aide de cette disposition. D'abord, la norme soulève la question de ce

					qu'il faut entendre par données personnelles secrètes (le lien qu l'on veut établir avec l'art. 321 CPS n'est compréhensible qu'à l'aide du rapport explicatif). Puis on doit se demander qui entre en ligne de compte comme auteur: s'agit-il de tout collaborateur d'une entreprise? S'agit-il aussi de collaborateurs de l'administration fédérale? Quelle serait alors la relation avec l'art. 320 CPS (secret de fonction)? Le but de la disposition doit faire l'objet d'une nouvelle analyse et il convient de la reformuler pour respecter l'exigence de la détermination de la formulation des normes pénales.
	LPD	53			Vu qu'il peut être difficile d'enquêter contre une personne déterminée à l'intérieur d'une entreprise, nous approuvons la possibilité de sanctionner l'entreprise comme telle. Toutefois, il n'y a aucune raison de réduire le montant maximal de l'amende.
	LPD	54			Cette disposition délègue la poursuite pénale des infractions contre le droit de la protection des données aux cantons (voir aussi remarques préliminaires aux art. 50-55 AP-LPD). De ce fait, les cantons devraient augmenter leurs ressources pour la mise en oeuvre de l'AP-LPD. De plus, au vu de la matière particulière que représente la protection des données, on doit craindre une application non unitaire des dispositions pénales en se fondant sur une juridiction cantonale. La mise en oeuvre de l'AP-LPD et donc la poursuite pénale y relative sont, de notre point de vue, affaire de la Confédération et celle-ci doit donc l'assumer.
	LPD	57			Cette disposition doit être supprimée. Depuis l'acceptation, par la Suisse, des accords Schengen-Dublin (accords d'association à Schengen) resp. au plus tard avec la mise en oeuvre de la nouvelle directive (UE) 680/2016 et lors de la ratification de la convention révisée STE 108, les cantons seront aussi tenus de garantir une protection adéquate des données personnelles et d'assurer cette protection par des autorités de surveillance indépendantes. Cette norme subsidiaire est donc obsolète et peut, sans autre, être supprimée.
	LPD	An.	Ch. 5		Art. 9 LTrans (RS 152.3). Complément: il convient d'actualiser le renvoi de l'art. 9 al. 2 LTrans à la LPD (art. 29 LPD au lieu de l'art. 19 LPD, actuellement prévu).

	LPD	An.	Ch. 10		Art. 1, deuxième phrase loi fédérale sur le traitement des données personnelles au Département fédéral des affaires étrangères (RS 235.2): Cpr. nos remarques relatives aux art. 3 lit. f et 27 al. 2 AP-LPD: dans le cadre du profilage, la loi doit contenir des garanties suffisantes pour la protection des droits fondamentaux de la personne concernée. Des blancs-seings (p.ex. «l'office fédéral est autorisé à traiter des données sensibles et à procéder à un profilage») ne suffisent en aucun cas. Nous proposons donc de prévoir, dans cette disposition, des restrictions suffisantes pour l'emploi du profilage.
	LPD	An.	Ch. 11		CPC (RS 272): Le CPC doit être complété de manière à ne pas exiger la prestation de sûretés ni de frais de procédure pour des actions et des requêtes relatives à la protection des données. En soi, ces allègements dans la conduite d'une procédure judiciaire par la personne concernée ne suffisent pas encore à abaisser l'obstacle existant pour la mise en oeuvre de la protection des données. Le manque d'efficacité des instruments de mise en oeuvre de la protection des données, constaté dans le rapport explicatif, ne peut être surmonté qu'à condition d'alléger, en outre, le fardeau de la preuve de la personne concernée. Dès lors, nous proposons un renversement du fardeau de la preuve pour les procédures de protection des données. En effet, compte tenu de la complexité du processus de traitement des données, la personne concernée n'est pas en mesure d'apporter la preuve d'un traitement de données illicite. Pour le responsable du traitement des données, un tel renversement du fardeau de la preuve ne signifie pas une aggravation de sa situation, dès lors qu'il est tenu, en vertu de l'art. 19 lit. a AP-LPD, de documenter son activité et ce indépendamment d'une procédure en cours.
	LPD	An.	Ch. 16		Art. 3 al. 2 LSIP (RS 361): Cpr. nos remarques relatives aux art. 3 lit. f et 27 al. 2 AP-LPD: dans le cadre du profilage, la loi doit contenir des garanties suffisantes pour la protection des droits fondamentaux de la personne concernée. Des blancs-seings (p.ex. «l'office fédéral est autorisé à traiter des données sensibles et à procéder à un profilage») ne suffisent en aucun cas. Nous proposons donc de prévoir, dans cette disposition, des restrictions suffisantes pour l'emploi du profilage.

	LPD	An.	Ch. 25		Art. 1 al. 1 LSIA (RS 510.91), phrase introductive: Cpr. nos remarques relatives aux art. 3 lit. f et 27 al. 2 AP-LPD: dans le cadre du profilage, la loi doit contenir des garanties suffisantes pour la protection des droits fondamentaux de la personne concernée. Des blancs-seings (p.ex. «l'office fédéral est autorisé à traiter des données sensibles et à procéder à un profilage») ne suffisent en aucun cas. Nous proposons donc de prévoir, dans cette disposition, des restrictions suffisantes pour l'emploi du profilage.
	LPD	An.	Ch. 28		Art. 71 al. 1 et 1bis LPPCi (RS 520.1): Cpr. nos remarques relatives aux art. 3 lit. f et 27 al. 2 AP-LPD: dans le cadre du profilage, la loi doit contenir des garanties suffisantes pour la protection des droits fondamentaux de la personne concernée. Des blancs-seings (p.ex. «l'office fédéral est autorisé à traiter des données sensibles et à procéder à un profilage») ne suffisent en aucun cas. Nous proposons donc de prévoir, dans cette disposition, des restrictions suffisantes pour l'emploi du profilage.
	LPD	An.	Ch. 35		Art. 107a al. 2 LA (RS 748.0): Cpr. nos remarques relatives aux art. 3 lit. f et 27 al. 2 AP-LPD: dans le cadre du profilage, la loi doit contenir des garanties suffisantes pour la protection des droits fondamentaux de la personne concernée. Des blancs-seings (p.ex. «l'office fédéral est autorisé à traiter des données sensibles et à procéder à un profilage») ne suffisent en aucun cas. Nous proposons donc de prévoir, dans cette disposition, des restrictions suffisantes pour l'emploi du profilage.

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

nom/société	remarque / suggestion :

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

nom/société	remarque / suggestion :

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions»)		
nom/société	**chap. n°**	**remarque / suggestion :**

Rapport explicatif : chap. 8 « Commentaire des dispositions »		
nom/société	**art.**	**remarque / suggestion :**

Amstutz Jonas BJ

Von: Stefan Thöni <stefan.thoeni@piratenpartei.ch>
Gesendet: Montag, 3. April 2017 20:09
An: Amstutz Jonas BJ
Cc: PPS Vorstand; David Herzog
Betreff: Vernehmlassungsantwort zum Vorentwurf der DSG-Totalrevision
Anlagen: Stellungnahme DSG Piratenpartei.doc; stefan_thoeni.vcf; signature.asc

Sehr geehrter Herr Amstutz

Im Namen der Piratenpartei Schweiz reiche ich hiermit die angehängte Vernehmlassungsantwort zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz ein.

--
Freundliche Grüsse
Stefan Thöni
Co-Präsident
Piratenpartei Schweiz

+41 79 610 64 95
@pirateexception

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Piratenpartei Schweiz

Abkürzung der Firma / Organisation : PPS

Adresse : Piratenpartei Schweiz, 3000 Bern

Kontaktperson : Stefan Thöni, Co-Präsident

Telefon : +41 79 610 64 95

E-Mail : stefan.thoeni@piratenpartei.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	Die Piratenpartei begrüsst grundsätzlich die überfällige Erneuerung des Datenschutzgesetzes, hält den Entwurf jedoch für unzureichend. Das Gesetz muss stark überarbeitet und verschärft werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	Das Recht auf Datenportabilität gehört untrennbar zur informationellen Selbstbestimmung und hat sehr weitgehenden Einfluss auf den Datenschutz, da es von Datenschutzproblemen betroffenen Personen ermöcht, den Anbieter einfach zu wechseln. Daher möchte die Piratenpartei die Datenportabilität analog zur DSGVO in DSG aufgenommen sehen.
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden	

werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	2			Es ist nicht einzusehen, weshalb bestimmte Behörden insgesamt vom Datenschutzrecht ausgenommen werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	2	2	b	Diese unberechtigte Ausnahme ist zu streichen. Soweit die Bundesversammlung Personendaten bearbeitet, soll dies explizit im Parlamentsgesetz erlaubt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	2	2	c	Diese unberechtigte Ausnahme ist zu streichen. Auch die Rechtsprechungstätigkeiten der Justizorgane sollen grundsätzlich dem Datenschutz unterliegen. Die notwendigen Erlaubsnistatbestände sollen im Prozessrecht (ZPO, StPO, VwVG, BGG, usw.) explizit kodifiziert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	2	2	d	Diese unberechtigte Ausnahme ist zu streichen. Speziell das IKRK bearbeitet besonders schützenswerte Personendaten und unterliegt ansonsten keinerlei Datenschutzbestimmungen.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	2	3		Diese unberechtigte Ausnahme ist zu streichen. Auch die Rechtsprechungstätigkeiten der Justizorgane sollen grundsätzlich dem Datenschutz unterliegen. Die notwendigen Erlaubsnistatbestände sollen im Prozessrecht (ZPO, StPO, VwVG, BGG, usw.) explizit kodifiziert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	2	4		Diese unberechtigte Ausnahme ist zu streichen. Auch die Rechtsprechungstätigkeiten der Justizorgane sollen grundsätzlich dem Datenschutz unterliegen. Die notwendigen Erlaubsnistatbestände sollen im Prozessrecht (ZPO, StPO, VwVG, BGG, usw.) explizit kodifiziert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3		c	Ziffer 4: Eindeutige Identifizierung eines Menschen durch biometrische Daten ist kaum möglich und daher als Kriterium ungeeignet. Stattdessen sollen alle biometrischen Daten erfasst werden, die bei der Identifizierung einer natürlichen Person hilfreich sein können. Dazu gehören insbesondere Fotos und Videos mit erkennbaren Gesichtern. Dies ist wichtig, weil Gesichtserkennung mittlerweile umfassend eingesetzt wird. Die Piratenpartei ist ausserdem der Auffassung, dass die Auflistung der besonders schützenswerden Personendaten lückenhaft ist. Dazu gehören müssten mindestens Kommunikationsinhalte, Foto-, Video- und Tonaufnahmen aus nichtöffentlichen Räumen, Bewegungsprofile, Beziehungsnetze und Online-Verlaufsprofile, da all diese Personendaten einen sehr weitgehenden Einblick in das Leben eines Menschen geben können.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	4			Eine freiwillige und informierte Zustimmung im bisherigen Rechtssinne ist nicht gut genug, da allenorts wesentliche Leistungen von der Zustimmung abhängig gemacht werden. Dies ist insbesondere bei Quasi-Monopolen ein grosses Problem. Deshalb ist folgender neuer Absatz einzufügen: "Die Einwilligung in die Datenbearbeitung ist nichtig, wenn eine Leistung davon abhängig gemacht wird, zu deren Erbringung die Einwilligung nicht zwingend erforderlich ist."

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	5	2		Auf die Feststellung des angemessenen Schutzes durch ausländische Gesetze durch den Bundesrat ist zu verzichten, da es sich hier nicht um eine politische Entscheidung handelt. Die Feststellung soll im Streitfall ein Gericht vornehmen. Zudem sollen konkrete Kriterien für einen minimalen Schutz wie z.B. allgemeines Verbot mit Erlaubnisvorbehalt, Rechtsschutz, usw. aufgeführt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	5	3-6		Absätze 3-6 sind zu streichen, da es keinen Ersatz für ausreichende gesetzliche Datenschutzbestimmungen im fremden Land gibt. Abkommen wie Privacy Shield, vertragliche Zusicherungen sowie unternehmensinterne Datenschutzvorschriften sind in jedem Fall ungenügend.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	6	1	b	Für die Erfüllung der meisten Verträge ist die Übermittlung in Staaten mit ungenügendem Datenschutzniveau nicht erforderlich. Der Nutzer soll sich darauf verlassen können, dass ohne seine explizite Einwilligung seine Daten nicht in solche Staaten exportiert werden. Dieser Buchstabe ist daher ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	**DSG**	6	1	**c**	Ziffer 1: Das öffentliche Interesse ist dahingehend zu präzisieren, dass z.B. fiskalische und wirtschaftliche Interessen der Schweiz nicht darunter fallen. Ziffer 2: Die Durchsetzung von Rechtsansprüchen in Ländern mit ungenügendem Datenchutzniveau muss hinter dem Datenschutzinteresse des Betroffenen zurückstehen. Daher ist diese Ziffer ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	6	1	e	Auch wenn der Betroffene die Daten selbst öffentlich macht, will er in der Regel nicht auf einen angemessenen Rechtsschutz, z.B. bezüglich Widerruf der Einwilligung oder Löschung und Korrektur der Daten, verzichten. Dieser Buchstabe ist daher ersatzlos zu streichen.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	6	1	f	Auch wenn die Daten in der Schweiz öffentlich zugänglich sind, will der Betroffene in der Regeln nicht auf den angemessenen Rechtsschutz, z.B. bezüglich Widerruf der Einwilligung, Löschung und Korrektur verzichten. Dieser Buchstabe ist daher ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	8-9			Die pauschalen Empfehlungen der guten Praxis sind zu streichen, da jeder Einzelfall anders ist und den Betroffenen nicht die Möglichkeit genommen werden darf, jeden Einzelfall umfassend gerichtlich beurteilen zu lassen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	11			Es braucht konkrete Mindeststandards für technische Sicherheitsmassnahmen, da diese immer noch von vielen Verantwortlichen vernachlässigt werden. Der Einsatz von Verschlüsselung zum Schutz der übertragenen und gespeicherten Personendaten ist angesichts der umfassenden Überwachung des Internets durch fremde Nachrichtendienste und Kriminelle zwingend notwendig. Deshalb sind folgende Absätze einzufügen: 1a "Nicht zur Veröffentlichung bestimmte Personendaten, ausgenommen diejenigen des Absenders und des Adressaten, dürfen ausschliesslich mit Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik geschützt über das Internet übertragen werden." 1b: "Nicht zur Veröffentlichung bestimmte Personendaten dürfen ausserhalb der geschützten Räumlichkeiten des Verantwortlichen oder des Datenverarbeiters nur auf nach dem Stand der Technik verschlüsselten Geräten und Speichermedien gelagert oder transportiert werden." 1c: "Wer behördlich oder gewerbsmässig Eingabe, Ansicht, Entgegennahme oder Versand von nicht zur Veröffentlichung bestimmten Personendaten über Internet anbietet muss die Verschlüsselung der Übertragung nach dem Stand der Technik auf allen von ihm verwendeten Kanälen ermöglichen. Davon ausgenommen sind Adresse und Name des Empfängers und Adressaten."

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	12	1-3		Das Opt-Out-Prinzip ist hier ungenügend, da so auch sensitive Daten möglicherweise in die Hände von aus Sicht des Verstorbenen nicht vertrauenswürdigen Angehörigen gelangen. Stattdessen soll hier ein Opt-In-Prinzip gelten, bei dem der Betroffene zu Lebzeiten eine Person oder mehrere Personen bezeichnen kann, welche nach seinem Tod Zugriff auf die Daten erhalten. Diese Personen müssen auch selbst kein schutzwürdiges Interesse haben, sondern sollen auch das Interesse des Verstorbenen wahrnehmen können.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13	2		Es sollen auch die Orte mitgeteilt werden, wo die Personendaten gespeichert und bearbeitet werden. Diese Information ist für die Beurteilung des Rechtsschutzes wesentlich. Zudem sollen auch die einzelnen Datenwerte inklusive Beschreibung mitgeteilt werden, damit der Betroffene den Umfang der Datenbearbeitung erkennen kann. Die Mitteilung ist zudem jährlich zu wiederholen, damit der Betroffenen einen Überblick über jeden Datenbearbeiter erhalten kann. Der Betroffene soll die fortlaufenden Mitteilungen auch abbestellen können (Opt-out).
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	14	1-2		Die Information ist auch dann wichtig, wenn der Betroffene bereits darüber verfügt oder verfügen könnte, um darauf aufmerksam zu machen, dass die Daten bearbeitet werden. Daher sind ist Absatz 1 und Absatz 2 lib. a zu streichen. Absatz 2 lit. b ist dahingehend einzuschränken, dass die Mitteilung nur unterbleiben kann, wenn keine Adresse erhoben wurde oder diese nicht mehr gültig ist.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	14	3		Litera b ist dahingehend einzuschränken, dass nur die identifizierenden Daten von Drittpersonen zurückgehalten werden. Dies ist für den Zweck, Drittpersonen zu schützen, ausreichend.
Fehler! Verweisquelle konnte	DSG	14	4		Für die Einschränkung nach Litera a ist kein Grund ersichtlich. Die Ausnahmen in Litera b sind in Bundesgesetzen (StPO, BWIS, usw.) explizit zu kodifizieren. Daher ist der ganze Absatz zu streichen.

nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	15			Die Piratenpartei begrüsst die Informations- und Anhörungspflicht bei automatisierten Einzelfallentscheidungen. Diese müsste jedoch noch weiter gehen und insbesondere dem Betroffenen Zugang zum Algorithmus und den Eingangsdaten gewähren, so dass er die Berechnung der Entscheidung nachvollziehen kann.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	15	3		Gerade wenn das Gesetz eine automatisierte Einzelfallentscheidung vorsieht, besteht ein erhöhtes Informations- und Anhörungsinteresse. Deshalb ist Absatz 3 ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	17			Die Piratenpartei begrüsst die Meldepflicht. Jedoch müsste in jedem Fall der Betroffene informiert werden, damit er seine Rechte selbstständig wahrnehmen und sich ggf. vor Folgen schützen kann, die der Verantwortliche nicht absehen kann.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	2		Die Auskunft muss auch die Rohdaten und eine verständliche Dokumentation umfassen, damit der Betroffene das Ausmass der Datenverarbeitung erkennen kann.
Fehler! Verweisquelle konnte nicht	DSG	23	2	c	Jede unbefugte Kenntnisnahme oder Bekanntgabe von Personendaten ist eine ist als Persönlichkeitsverletzung zu sehen. Litera c ist ensprechend zu ergänzen.

gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	24	2	c	Kreditwürdigkeitsprüfungen fallen vor allem durch massenhaften Missbrauch auf und sind daher als Rechtfertigungsgrund ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	25	4		Schäden aus Persönlichkeitsverletzung wegen Datenschutzverstässen sind häufig schwer monetär zu erfassen und noch schwerer zu beweisen. Deshalb soll jede solche Persönlichkeitsverletzung eine Genugtuungsanspruch von 50 bis 1000 Franken begründen. Um damit Freizeitvereine nicht zu gefährden soll es für nichtkommerzielle Verantwortliche Ausnahmen geben können. Der neue Absatz im Wortlaut: "Der von einer rechtswidrigen Verletzung seiner informationellen Selbstbestimmung betroffene hat jedenfalls Anspruch auf eine Genugtuung von 50 bis 1000 Franken. Der Richter kann den Genugtuungsanspruch reduzieren oder verneinen, wenn die Verletzung nicht von einem Gewerbebetrieb ausging."
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	25	5		Wie bereits beim bestehenden Datenschutzrecht ist die Rechtsdurchsetzung nach dem Entwurf weiterhin ein Problem, da oft viele Konsumenten oder Arbeitnehmer betroffen sind, die sich gegenüber dem Verantwortliche in einer schwachen Position befinden. Aus diesem Grund ist analog zu Art. 10 Abs. 2 UWG eine Verbandsklagerecht einzuführen. Aus denselben Gründen soll die kollektive Rechtsdurchsetzung gegenüber Bundesbehörden durch ein Verbandsbeschwerderecht gegeben werden. Die kollektive Rechtsdurchsetzung auf eine spätere Gesamtlösung zu vertagen ist für die Piratenpartei angesichts der besonderen Schwierigkeiten im Datenschutzrecht keine Option. Der neue Absatz im Wortlaut: "Das Klagerecht steht auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss dem Datenschutz, Kosnumentenschutz oder Arbeitnehmerschutz widmen zu."
Fehler! Verweisquel	DSG	25	6		Die Piratenpartei wünscht sich in Gerichtsverfahren wegen Datenschutzverletzungen eine Beweislastumkehr sobald eine Datenschutzverletzung glaubhaft gemacht wurde. Dies ist notwendig, da sich

le konnte nicht gefunden werden.					Datenschutzverletzungen vielfach aus internen Abläufen und mangelhaften technischen Vorkehren des Verantwortlichen ergeben, die durch den Kläger nur in sehr aufwendigen Beweisverfahren zu beleuchten sind. Der neue Absatz im Wortlaut: "Wird eine Datenschutzverletzung durch den Kläger glaubhaft gemacht, so hat der Beklagte zu Beweis über die rechtmässige Datenverarbeitung zu erbringen."
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	28			Die Piratenpartei lehnt datenschutzrelevante Experimente ohne explizite gesetzliche Grundlage ab. Daher ist dieser Artikel zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	29	2	e	Die Bundesbehörden sollen nicht Gehilfen für die Durchsetzung zivilrechtlicher Ansprüche sein. Deshalb ist dieses Literal ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	29	4		Alleine die Auflistung von Namen und Geburtsdaten in einem bestimmten Kontext kann zu einer schweren Persönlichkeitsverletzung führen, so zum Beispiel Listen von Bundesangestellten, Sicherheitsüberprüften, usw. Zudem ist auch die Adresse sensitiv, da damit unerwünschte Werbung zugestellt oder Personen unerwünscht zuhause aufgesucht werden können. Aus diesen Gründen ist dieser Absatz ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	30	1		Jede Person hat ein inhärentes Interesse an informationeller Selbstbestimmung. Auf ein darüber hinausgehendes Interesse ist deshalb zu verzichten.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	37	1		Der Beauftragte sollte von der Exektuive möglichst unabhängig sein und deshalb direkt von Parlament gewählt werden. Das Amt ist zudem jeweils auszuschreiben und alle grundsätzlich geeigneten Bewerber sind in öffentlicher Sitzung der Bundesversammlung anzuhören.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52	1		Der Geheimnisbegriff erscheint hier zu stark. Es muss ausreichen, dass die Daten ohne gesetzliche Grundlage an jemanden weitergegeben wurden, der die Daten nicht zur zweckgemässen Bearbeitung kennen musste.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52	1	a	Hier scheint eine Gesetzeslücke für ehrenamtliche Tätigkeiten bspw. für Kirchen, Vereine und politische Parteien zu bestehen. Diese Tätigkeiten sind mit zu erfassen: "von denen er im Rahmen seiner beruflichen oder ehrenamtlichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat;"
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52	3		Der Wortlaut ist hier ebenfalls auf die ehrenamtlich tätigen Personen auszudehnen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52			Es sollte ein qualifiziertes Delikt für den Fall von besonders schützenswerten Personendaten oder Personendaten einer grossen Anzahl Menschen vorgesehen werden.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	53			Die meisten Datenschutzverletzungen gehen von schlechten Geschäftspraktiken oder systematisch ungenügenden Vorkehrungen in Unternehmen aus. Deshalb ist eine primäre Strafbarkeit der Unternehmen nach Verwaltungstrafrecht vorzuziehen und die Strafen direkt durch den EDÖB auszusprechen. Zudem muss die Höhe der Strafen so bemessen sein, dass sich Datenschutzverletzungen für Unternehmen niemals lohnen. Eine Übernahme der Strafhöhen der EU-DSGVO von bis 20 Millionen Euro oder 4% des Jahresumsatzes erscheint angemessen.
Fehler! Verweisquelle konnte nicht gefunden werden.	ZGB	45a	3		Ziffer 3: Die Piratenpartei regt an, die Aufsichtsinstanz direkt im Gesetz zu regeln. Geeignet halten wir dafür einzig den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).
Fehler! Verweisquelle konnte nicht gefunden werden.	ZPO	114			Dass die Kläger von den Gerichtskosten befreit werden sollen, ist sehr zu begrüssen. Jedoch schrecken drohende hohe Parteikosten potenzielle Kläger weiterhin ab. Daher schlagen wir vor, zudem die Höhe der Parteikosten so zu begrenzen, dass berechtigte Ansprüche ohne finanzielle Hürden eingeklagt werden können.
Fehler! Verweisquelle konnte nicht gefunden werden.	StGB	179decies			Die Piratenpartei begrüsst ausdrücklich den neuen Straftatbestand des Identitätsmissbrauchs und den Wortlaut des Artikels. Es fragt sich jedoch, ob nicht auch unter Strafe gestellt werden muss, wenn durch Identitätsmissbrauch Dritte zu Schaden kommen.
Fehler! Verweisquelle konnte nicht gefunden	StGB	143bis			Zusätzlich zu den Straftatbeständen in Art. 143bis hält es die Piratenpartei für erforderlich, auch das Hinterlassen einer offenen Sicherheitslücke (Backdoor) unter Strafe zu stellen. Wenn beim Eindringen (oder einem Versuch) in ein Datenverarbeitungssystem das Zielsystem für Dritte leichter angreifbar gemacht wird, kann sich der Schaden multiplizieren.

werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	StGB				Zudem sollte unter Strafe gestellt werden, wenn heimlich und mittels Gerät über Personen Daten gesammelt werden, z.B. indem ein Fahrzeug versteckt mit einem GPS-Tracker ausgestattet wird.
Fehler! Verweisquelle konnte nicht gefunden werden.	StGB				Unter Strafe gestellt werden soll ausserdem das Verbreiten und Publizieren nichtöffentlicher Kommunikation wie z.B. Chatnachrichten, SMS, usw., da dies dem Verbreiten und Publizieren nichtöffentlicher Gesprächen gemäss Art. 179ter Abs. 2 StGB entspricht und Chatnachrichten heute meist analog zu Telefongesprächen eingesetzt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht	

gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Beat.Rudin@dsb.bs.ch
Gesendet: Freitag, 17. März 2017 16:10
An: Amstutz Jonas BJ
Betreff: Totalrevision DSG: Stellungnahme von privatim
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_DE_(privatim)_20170309.doc; Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_DE_(privatim)_20170309.pdf
Signiert von: beat.rudin@dsb.bs.ch

Wichtigkeit: Hoch

Sehr geehrter Herr Amstutz

Wir danken Ihnen für die Einladung, uns zum Entwurf für die Totalrevision des Datenschutzgesetzes vernehmen zu lassen. Gerne lassen wir Ihnen in der Beilage die Stellungnahme von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, zum VE-DSG zukommen (PDF- und Word-Dokument). Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Wir danken für die Berücksichtigung unserer Anliegen und sind gerne bereit, Sie weiter zu unterstützen.

Freundliche Grüsse
Beat Rudin

_____
privatim *Die schweizerischen Datenschutzbeauftragten / Les préposé(e)s suisses*
à la protection des données / Gli incaricati svizzeri della protezione dei dati
Beat Rudin, Präsident
c/o Datenschutzbeauftragter des Kantons Basel-Stadt
Henric Petri-Strasse 15, Postfach 205, CH-4010 Basel
Tel. +41 (61) 201 16 40, Fax +41 (61) 201 16 41
E-Mail beat.rudin@dsb.bs.ch und praesident@privatim.ch
Website http://www.privatim.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation	: privatim, Vereinigung der schweizerischen Datenschutzbeauftragten
Abkürzung der Firma / Organisation	: privatim
Adresse	: c/o Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, 4010 Basel
Kontaktperson	: Beat Rudin
Telefon	: 061 201 16 42
E-Mail	: beat.rudin@dsb.bs.ch
Datum	: 09.03.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Im Zentrum der Totalrevision des DSG steht die Stärkung der Wirkung des Gesetzes und der Rechte der betroffenen Personen. Dabei lässt sich die Reform sehr stark von den Entwicklungen auf europäischer Ebene leiten. In Bezug auf die Stärkung der Rechte der betroffenen Personen werden indessen zwei zentrale Elemente der EU-Reform ignoriert: Art. 20 Verordnung (EU) 2016/679 sieht ein Recht auf Datenübertragbarkeit vor und Art. 17 Verordnung (EU) 2016/679 ein Recht auf Löschung («Recht auf Vergessenwerden»). Beide Rechte stärken die Position der betroffenen Personen insbesondere gegenüber grossen global tätigen Datenbearbeitern. Es ist nicht nachzuvollziehen, warum den Schweizer Bürgerinnen und Bürger ein solches Recht verwehrt werden soll. Wir empfehlen deshalb, die Aufnahme dieser beiden Rechtsinstrumente in die Totalrevision des DSG ernsthaft zu prüfen.
	Wir beantragen eine Aufteilung des bisherigen Bundesdatenschutzgesetzes in *zwei Erlasse*: ein *Datenschutzgesetz für private Datenbearbeiter* und *eines für die Bundesorgane*. Eine solche Aufteilung macht Sinn, ● weil sich die *Rechtfertigungskonzepte* in den beiden Bereichen entscheidend unterscheiden (öffentlichrechtlich: Legalitätsprinzip / privatrechtlich: Einwilligung, überwiegendes Interesse, Gesetz), was (auch schon in der Vergangenheit) die Regulierung in den allgemeinen Grundsätzen (für beide Bereiche) und besonderen Bestimmungen (je für einen Bereich) kompliziert und schwerfällig machen, und ● weil damit die *Frist* zur Umsetzung der schengen-relevanten Richtlinie (EU) 2016/680 wohl eingehalten werden könnte. Ausserdem könnte damit für die Zukunft *zwei Handlungsoptionen offengehalten* werden: ● Einerseits könnten mittelfristig – wie in vielen Kantonen mit dem Öffentlichkeitsprinzip – die Regelung des *Datenschutzes und* des *Öffentlichkeitsprinzips* als zwei Seiten derselben Medaille *in einem Gesetz* zusammengeführt werden. ● Andererseits könnte längerfristig, nachdem dafür die notwendige Verfassungsgrundlage geschaffen worden ist, ein *einheitliches, schweizweit geltendes Datenschutzgesetz für alle öffentlichen Organe* geschaffen werden. Damit müssten auch nicht mehr bei jeder Änderung des übergeordneten internationalen Rechts das Bundesdatenschutzgesetz und 26 kantonale Datenschutzgesetz angepasst werden, was erfahrungsgemäss (wie auch dieses Mal) zeitlich äusserst anspruchsvoll ist, weil die Kantone faktisch abwarten müssen, wie der Bund die

	geforderten Anpassungen umsetzt.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
	DSG	1			Einverstanden mit Beschränkung auf den Schutz natürlicher Personen,
	DSG	2	2	c	Der Ausschluss der Rechtsprechung entspricht nicht dem Übereinkommen SEV 108, das keine Möglichkeiten zur Ausnahme vom Geltungsbereich vorsieht. Wir schlagen folgende Regelung vor: Geltungsbereich des DSG (d.h. die Grundsätze, z.B. betreffend Informationssicherheit, Vorabkonsultation usw.) auch für die Rechtsprechungsorgane. Die Prozessordnungen gelten als bereichsspezifisches Datenschutzrecht (d.h. lex specialis) ohnehin (vgl. dazu Beat Rudin, Überholte Ausnahmen im Geltungsbereich, digma 2016, 122 ff.). Einzig zwei Ausnahmen sind erforderlich (und konventionskonform) (und werden auch von der Konferenz der Kantonsregierungen in ihrem Leitfaden für die Anpassung der kantonalen Datenschutzgesetze so empfohlen): ● Damit nicht die Rechte der betroffenen Personen und die Parteirechte der Prozessrechte kollidieren: Es kann (in Art. 2 VE-DSG) festgelegt werden, dass sich während der Hängigkeit eines gerichtlichen Verfahren die Ansprüche und Rechte der betroffenen Personen ausschliesslich nach dem anwendbaren Verfahrensrecht richten, so dass in dieser Phase die Parteien z.B. nur ihr verfahrensrechtliches Akteneinsichtsrecht geltend machen können, nicht aber ihr datenschutzrechtliches Recht auf Auskunft (auf Zugang zu den eigenen Personendaten). ● Damit nicht Aufsichtsrechte/-pflichten kollidieren: Es kann (z.B. in Art. 40 VE-DSG) festgelegt werden, dass die Datenbearbeitungen in hängigen gerichtlichen Verfahren vor eidgenössischen Gerichten von der Aufsicht durch den EDÖB ausgenommen sind.

	DSG	2	3		Siehe Bemerkung zu Art. 2 Abs. 2 lit. c VE-DSG Ausserdem: Sollen die Gerichte (ausserhalb ihrer Rechtsprechungstätigkeit) von der Aufsicht durch den EDÖB generell ausgenommen sein oder soll er ihnen gegenüber bloss (wie von der Konferenz der Kantonsregierungen in ihrem Leitfaden im Leitfaden für die Umsetzung in den kantonalen DSG vorgeschlagen) bloss keine Anordnungen treffen können? Wir beantragen zweiteres.
	DSG	3		a	Ziff. 2: Wir begrüssen die Aufnahme des Kriteriums «Ethnie» (Zugehörigkeit zu einer Gruppe von Menschen, die sich aufgrund ihrer Kultur, Geschichte, Sprache, Sitten, Traditionen und Gebräuche als untereinander verbunden und dadurch als von der übrigen Bevölkerung differente Gemeinschaft erleben und/oder von der übrigen Bevölkerung als differente Gruppe wahrgenommen werden). Demgegenüber beantragen wir die Streichung des Begriffs «Rasse». «Rasse» ist in Bezug auf die Menschen kein wissenschaftlicher Begriff; geschützt werden soll vielmehr vor dem Rassevorwurf (historisch: «Jude», «Neger» usw.).
	DSG	3		c	Ziff. 3: Wir begrüssen die Aufnahme des Begriffs «genetische Daten» in die besonders schützenswerten Personendaten.
	DSG	3		c	Ziff. 4: Der Begriff der biometrischen Daten ist missverständlich. Auch in den Erläuterungen wird er nicht geklärt: Ein Gesichtsbild (ein Portrait) ist grundsätzlich auch ein «biometrisches Datum», soll aber hier nicht als Unterkategorie der besonders schützenswerten Personendaten erfasst werden. Wir beantragen deshalb (wie auch die Konferenz der Kantonsregierungen in ihrem Leitfaden für die Anpassung der kantonalen Datenschutzgesetze), die folgende Definition aufzunehmen: «4. mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Peron ermöglichen oder bestätigen (biometrische Daten)».

	DSG	3		d	Der Begriff «Speichern» widerspricht dem Anliegen der technikneutralen Formulierung des Gesetzes.
	DSG	3		d	In der Vernehmlassungsvorlage (Art. 4 Abs. 5, Art. 25 Abs. 1, Art. 29 und 30) und auch in der Richtlinie (EU) 2016/680 werden die Begriffe «Löschen» und «Vernichten» nebeneinander verwendet, ohne dass das Verhältnis der beiden zueinander geklärt wird. Vernichten hat bisher das endgültige physische «Zerstören» gemeint. Ob Löschen nur das «Entfernen aus dem aktiven Prozess» (ähnlich wie das Löschen von Strafregistereinträgen) meint oder einfach das Vernichten im elektronischen Umfeld umschreibt, muss festgelegt werden. Wir beantragen deshalb eine Klärung im Gesetzestext oder mindestens im Botschaftstext.
	DSG	3		f	Wir begrüssen den Ersatz des bis heute unklaren Begriffs des «Persönlichkeitsprofils» (als «gefährliche» Art von *Daten*) durch das «Profiling» (als «gefährliche» Art des *Bearbeitens* von Daten). Allerdings ist es völlig ungenügend, wenn dann im bereichsspezifischen Datenschutzrecht (in den anzupassenden Bundesgesetzen) mit Blankettnormen das Profiling quasi «durchgewinkt» wird. Verlangt ist, dass klare und strenge Rahmenbedingungen für das Profiling in den Bundesgesetzen konkretisiert werden.
	DSG	3		i	Wir beantragen, im schweizerischen Recht vom «Auftrags*daten*bearbeiter» zu sprechen. Diese Person/Stelle muss nicht einfach einen Auftrag bearbeiten, sondern im Auftrag des Verantwortlichen Daten bearbeiten. Eine Abweichung vom Begriff im europäischen Recht ist problemlos möglich, da mit dem *Be*arbeiter (anstelle des *Ver*arbeiters) ohnehin schon – und zu Recht – von der europäischen Begrifflichkeit abgewichen wird. Ausserdem verwendet der VE-DSG den Begriff der Auftrags*daten*bearbeitung auch schon in der Überschrift von Art. 7.
	DSG	3			Wir begrüssen die Streichung des Begriffs der «Datensammlung», da dieser Begriff im Zeitalter der Digitalisierung völlig veraltet ist und an etwas anknüpft, das im modernen IT-Umfeld längst nicht mehr gegeben ist.

	DSG	4	4		Wir begrüssen grundsätzlich die Neuformulierung und Ergänzungen von Art. 4 DSG. Zu Art. 4 Abs. 4 VE-DSG ist festzustellen, dass die Festlegung von Aufbewahrungsfristen impliziert wird. Diese Pflicht der Verantwortlichen sollte mindestens im Botschaftstext zum Ausdruck kommen.
	DSG	4	6		Es ist zu begrüssen, dass bei der Einwilligung festgehalten wird, dass sie nicht nur freiwillig, sondern auch *eindeutig* zu erfolgen hat. Im 2. Satz sollte aber auch der Begriff „ausdrücklich“, dessen Bedeutung bisher in der Literatur kontrovers diskutiert wurde, mindestens durch eine Erläuterung im Botschaftstext geklärt werden.
	DSG	7			Die Bestimmung übernimmt weitgehend die Formulierung von Art. 10a DSG. Allerdings kommen dadurch die europarechtlichen Vorgaben (insbesondere aus der Richtlinie (Art. 22 f. RL (EU) 2016/680) für die Bundesorgane) nicht korrekt zum Ausdruck. In Bezug auf die Begriffe sollte analog zur Überschrift auch im Text vom Auftrags*daten*bearbeiter gesprochen werden (siehe auch unsere Bemerkung zu Art. 3 lit. i VE-DSG)
	DSG	7	1	a	Der Verantwortliche muss sich nicht nur vergewissern, dass die Datensicherheit und die Rechte der betroffenen Personen gewährleistet sind, sondern *er muss wirksam sicherstellen,* dass die Daten nur so bearbeitet werden, wie der Verantwortliche es selber tun darf. Entsprechend ist die Formulierung in lit. a zu ergänzen.
	DSG	7	2		Art. 7 Abs. 2 VE-DSG ist in Abhängigkeit von der Anpassung in lit. a neu zu formulieren. Zudem sollte der Bundesrat nicht Anforderungen an den Auftragsdatenbearbeiter präzisieren, sondern die Verantwortlichen in die Pflicht nehmen, indem die einzelnen Anforderungen an die Auswahl des Dritten und die Sicherstellung, dass die Personendaten nur so bearbeitet werden, wie es der Verantwortliche tun dürfte, auf Verordnungsstufe detailliert geregelt werden
	DSG	8			Das neue Instrument der Empfehlungen der guten Praxis, wobei der Beauftragte solche zu erarbeiten oder

					zu genehmigen hat, ist kritisch zu beurteilen. Dieses Instrument braucht bedeutende Ressourcen, um zum richtigen Zeitpunkt zusammen mit den interessierten Kreisen und unter Berücksichtigung der Besonderheiten eines Anwendungsbereichs über Empfehlungen zu verfügen, die in der Praxis auch Wirkung erzielen können. Solange nicht geklärt ist, wie diese Ressourcen dem Beauftragten zur Verfügung gestellt werden, erscheint dieses Instrument als wirkungslos.
	DSG	8	1		Es ist zu präzisieren, dass es sich bei der Konkretisierung um die Datenschutzvorschriften *des Bundesrechts* handelt. Sofern Empfehlungen der guten Praxis auch den öffentlich-rechtlichen Bereich betreffen sollen, ist ihre Anwendbarkeit auf die Bundesorgane zu beschränken oder allenfalls eine Zusammenarbeit mit den kantonalen Datenschutzaufsichtsbehörden zu suchen. Dies sollte mindestens im Botschaftstext präzisiert werden.
	DSG	9	1+2		Der Wortlaut von Art. 9 VE-DSG bringt zu wenig zum Ausdruck, dass es sich bei der Einhaltung der Empfehlungen der guten Praxis lediglich um eine gesetzliche Vermutung der Einhaltung der Datenschutzvorschriften handelt. Da es sich aber generell bei den Empfehlungen der guten Praxis um eine Konkretisierung des Gesetzes handeln soll und die Empfehlungen nie die Konkretsierung des gesamten Gesetzes umfassen können, trägt diese gesetzliche Vermutung auch nur einen Teil zur Gesamtbeurteilung bei, ob eine Datenbearbeitung die Datenschutzvorschriften einhält. Dies wird auch dadurch unterstrichen, dass die Einhaltung der Empfehlungen der guten Praxis freiwillig ist (Abs. 2). Aus diesem Grund könnte Art. 9 VE-DSG ersatzlos gestrichen werden, ohne dass dies die Wirkung des Gesetzes beeinträchtigen würde.
	DSG	10			In den Erläuterungen zu Art. 10 VE-DSG wird darauf verwiesen, dass keine Änderungen zum bisherigen Art. 11 DSG bestehen, obwohl Art. 10 VE-DSG nur noch von «Datenbearbeitungsvorgängen» spricht, im Gegensatz zu Art. 11 DSG, der auch die «Datenbearbeitungssysteme und –programme» (Produkte) explizit erwähnt. Diese Änderung des Wortlauts deckt sich nicht mit den Erläuterungen, die davon ausgehen, dass die Produkte auch mitenhalten seien. Dabei ist in Art. 10 VE-DSG die Zertifizierung nur noch für Verantwortliche oder Auftrags(daten)bearbeiter möglich, was gerade die Hersteller von Produkten ausschliesst. Da die Poduktezertifizierung auch nach dem bisherigen Recht toter Buchstabe geblieben ist,

					kann sie durchaus ausgeschlossen werden, was aber zumindest im Botschaftstext klar festzuhalten wäre.
	DSG	11			Art. 11 VE-DSG orientiert sich zu stark am bisherigen Art. 7 DSG und unterlässt es, Schutzziele zu definieren wie dies Art. 32 Abs. 1 lit. b Verordnung (EU) 2016/679 und Art. 29 Abs. 2 Richtlinie (EU) 2016/680 tun, aber auch in modernen kantonalen Datenschutzgesetzen zu finden sind (z.B.: § 7 IDG/ZH, § 8 IDG/BS). Dabei ist auch der veraltete Begriff des «unbefugten Bearbeitens» zu hinterfragen. Zudem sind Massnahmen gegen das «unbefugtes Bearbeiten» und den «Verlust» zu treffen. (Das «oder» als Alternative wäre falsch). Wir schlagen deshalb vor, die Schutzziele explizit im Gesetz zu erwähnen.
	DSG	12			Wir begrüssen grundsätzlich, dass eine Regelung für den Zugang zu Daten einer verstorbenen Person vorgesehen wird. Allerdings haben wir Zweifel, ob die vorgeschlagene Lösung den Sachlage gerecht wird. Eine Untersagung i.S.v. Art. 12 Abs. 1 lit. a VE-DSG wird im Alltag kaum je vorkommen. Somit hängt die Entscheidung allein an einer Interessenabwägung nach Art. 12 Abs. 1 lit. b VE-DSG, allerdings mit der Schwierigkeit, dass die abzuwägenden Interessen der verstorbenen Person durch den Datenbearbeiter, der Einsicht geben soll, schwer zu ermitteln und zu gewichten sind (wenn man nicht davon ausgeht, dass mit dem Tod die Interessen der verstorbenen Person ohnehin «untergehen»). Wir beantragen deshalb, zu prüfen, ob die Norm nicht restriktiver ausgestaltet werden muss.
	DSG	12	3		Die Ausschaltung des Amtsgeheimnisse (insbesondere der besonderen Amtsgeheimnisse, also nicht bloss des personalrechtlichen) und der Berufsgeheimnisses einzig aufgrund einer Interessenabwägung (Art. 12 Abs. 1 VE-DSG) erscheint uns problematisch. Der Weg, aus solchen Schweigeverpflichtungen «herauszukommen», ist die Entbindung durch die Aufsichtsbehörde. Wir beantragen, diesen Absatz zu streichen oder restriktiver zu formulieren.
	DSG	15			Von Bedeutung ist diese Regelung v.a. im *Privatrecht*. Für diesen Bereich wird sie begrüsst. Im *öffentlichen Recht* ergehen Einzelentscheidungen mit rechtlichen Wirkungen in aller Regel in Form der *Verfügung*. Weil diese *eröffnet* werden müssen, ist die Information der betroffenen Personen sichergestellt.

					Weil den betroffenen Personen im Vorfeld des Erlasses von Verfügungen ein Anspruch auf *rechtliches Gehör* zukommt, ist auch sichergestellt, dass die betroffenen Personen sich zur Einzelentscheidung äussern können. Aus diesem Grund geht der KdK-Leitfaden für die Umsetzung in den kantonalen DSG davon aus, dass es keine spezifische Regelung in den kantonalen (Informations- und) Datenschutzgesetzen braucht. Wir beantragen deshalb zum einen, die Regelung (ohne Abs. 3) in den Abschnitt zum Datenbearbeiten durch Private zu verschieben. Wir beantragen zum andern, dass im öffentlichrechtlichen Bereich automatisierte Einzelentscheidungen, die nicht in Form einer Verfügung eröffnet werden, ausschliesslich zuzulassen sind, wenn ● ein Gesetz (im formellen Sinn) dies ausdrücklich vorsieht und ● das Gesetz gleichzeitig geeignete Massnahmen zum Schutz der Rechte der betroffenen Personen (insbesondere bezüglich der Transparenz und Einwirkungsmöglichkeiten für die betroffenen Personen) vorsieht.
	DSG	16			Wir beantragen, die Datenschutz-Folgenabschätzung (Art. 16 Abs. 1 und 2 VE-DSG) und die Vorabkonsultation (Art. 16 Abs. 3 und 4 VE-DSG) in zwei separaten Artikeln zu regeln und das Instrument der Vorabkonsultation als wirksamstes Mittel des präventiven Datenschutzes (mindestens bei Datenbearbeitungen von Bundesorganen) obligatorisch zu erklären, wenn diese zu einem erhöhten Risiko für die Persönlichkeit oder für die Grundrechte der betroffenen Personen führen.
	DSG	16	1+2		Eine Datenschutz-Folgenabschätzung hat *bei jedem Vorhaben einer Datenbearbeitung* stattzufinden. Was hier als Voraussetzung formuliert wird («voraussichtlich zu einem erhöhten Risiko führt»), ist bereits das Resultat eines ersten Schritts der Folgenabschätzung. Diese Datenschutz-Folgenabschätzung ist im Grunde genommen nichts anderes als die Vorbereitung des Verantwortlichen, damit er die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften (Art. 19 lit. a VE-DSG) erbringen kann. Ausserdem beschlägt sie dieselben Punkte, die bei Vorhaben, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, für eine Vorabkonsultation (Art. 16 Abs. 3 und 4 VE-DSG)

					erarbeitet werden müssen.
	DSG	16	3+4		Die Vorabkonsultation, wie sie von Art. 8bis Ziff. 2 des Übereinkommens SEV 108 und von Art. 28 der Richtlinie (EU) 2016/680 verlangt wird, wird vom Bund in Art. 16 Abs. 3 und 4 VE-DSG ungenügend umgesetzt. Die Vorabkonsultation (oder Vorabkontrolle, wie sie bei den bisher geltenden europarechtlichen Vorgaben hiess) hätte vom Bund bereits bei der Schengen-Assoziierung eingeführt werden müssen. Sie ist eines der wirksamsten Mittel des präventiven Datenschutzes, wie die verbreitete Praxis bei den Kantonen beweist. Wir beantragen deshalb, dass dann, wenn die Datenschutz-Folgenabschätzung ein erhöhtes Risiko* für die Persönlichkeit (bei privatrechtlichem Datenbearbeiten) oder für die Grundrechte der betroffenen Personen (bei öffentlichrechtlichem Datenbearbeiten) ergibt, das Ergebnis zusammen mit den vorgesehenen Massnahmen – mindestens bei Vorhaben der Bundesorgane – zwingend dem Beauftragten zur Vorabkonsultation vorzulegen ist; er hat dann zu prüfen, ob die Verantwortlichen die Risiken für die Grundrechte der betroffenen Personen nicht hinreichend ermittelt oder durch die vorgeschlagenen Massnahmen nicht hinreichend eingedämmt hat. *Art. 28 der Richtlinie (EU) 2016/680 spricht von hohem Risiko; das entspricht in der Terminologie beispielsweise des in der Schweiz verbreitet angewandten Grundschutz-Konzeptes des (deutschen) Bundesamtes für die Sicherheit in der Informationstechnologie/BSI einem erhöhten Risiko, das z.B. besteht, wenn besonders schützenswerte Personendaten bearbeitet werden; ein erhöhtes Risiko verlangt über den Grundschutz hinaus spezifisch nach besonderen Schutzmassnahmen. Ein hohes Risiko verlangt schon fast Hochsicherheitsmassnahmen und trifft nur für sehr wenige Anwendungen zu.
	DSG	17	1		Die «Verletzung des Datenschutzes» wird in Art. 17 Abs. 1 VE-DSG nicht klar definiert, was aber auch im Hinblick auf die mögliche Strafbarkeit des Verantwortlichen (siehe Art. 50 Abs. 2 lit. e und Art. 50 Abs. 3 lit. b VE-DSG) unentbehrlich ist (siehe hierzu unsere Ausführungen zu Art. 50 ff. VE-DSG). Die Defintion ist entweder in diesem Artikel oder unter den Begriffen (Art. 3 VE-DSG) nachzutragen. Dabei schlagen wir vor, die Defintion gemäss dem KdK-Leitfaden für die Umsetzung in den kantonalen DSG zu formulieren: «Eine

					Datenschutzverletzung liegt vor, wenn die Sicherheit so verletzt wird, dass bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten.» Die Meldepflicht soll entfallen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt. Diese Formulierung lässt dem Verantwortlichen einen weiten Ermessensspielraum, der faktisch die vorsätzliche oder fahrlässige Strafbarkeit der Nichtmeldung ausschliesst. Der Ermessensspielraum ist deshalb konkreter einzuschränken und die Anwendung des Strafrechts zu überdenken (siehe hierzu unsere Ausführungen zu Art. 50 ff. VE-DSG).
	DSG	18	1		Aus der Formulierung von Art. 18 Abs. 1 VE-DSG wird nicht klar, wie weit hier eine Verpflichtung der Verantwortlichen entstehen soll, die nicht bereits aufgrund von Art. 11 VE-DSG besteht. Fragwürdig erscheint deshalb auch die mögliche strafrechtliche Sanktionierung der Unterlassung von Massnahmen gemäss Art. 18 VE-DSG (Art. 51 Abs. 1 lit. e VE-DSG). «Datenschutz durch Technik» ist eine mögliche Massnahme aufgrund der Vorgaben von Art. 11 VE-DSG und daher Teil eines gesamten Massnahmenpakets gestützt auf Art. 11 VE-DSG. Abs. 1 ist deshalb mit Art. 11 VE-DSG zusammenzuführen.
	DSG	18	2		Wie bereits in den Erläuterungen angetönt, ist Art. 18 Abs. 2 nur für den privatrechtlichen Teil sinnvoll, da Bundesorgane Daten nur aufgrund einer Rechtsgrundlage bearbeiten (Art. 27 VE-DSG). Die Formulierung ist deshalb entsprechend anzupassen. Zudem könnte Abs. 2 auch in Zusammenhang mit Art. 4 VE-DSG eingeordnet werden.
	DSG	19	1		Entgegen den Ausführungen in den Erläuterungen, ist festzuhalten, dass die in lit. a statuierte Dokumentationspflicht den Anforderungen von Art. 8^{bis} Ziff. 1 E-Übereinkommen SEV 108 und Art. 4 Abs. 4 RL 2016/680 nicht entspricht. Vilemehr müssen der Verantwortliche und der Auftrags(daten)bearbeiter *nachweisen* können, dass sie die Datenschutzbestimmungen einhalten. Dies geht über ein Register der

					Datenbearbeitungen hinaus. Dieser Nachweis kann in einem Datenschutzmanagementsystem (DSMS) erbracht werden. DSMS basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Wird auf eine diesbezügliche Zertifizierung verzichtet, ist festzulegen, welche Dokumente notwendig sind, um diesen Nachweis erbringen zu können (z.B. Informationssicherheitskonzept, Zugriffskonzept usw.). Hierzu bestehen bereits zahlreiche Hilfsmittel. Es ist sinnvollerweise auf Verordnungsstufe festzulegen, in welchen Fällen ein solches DSMS obligatorisch sein soll (z.B. nur wenn besonders schützenswerte Personendaten bearbeitet werden). Eine klare Regelung ist zudem erforderlich, da das Fehlen einer Dokumentation strafrechtlich sanktioniert werden soll (Art. 51 Abs. 1 lit. f VE-DSG), was nur bei einer genügenden Bestimmtheit der Strafnorm möglich ist (siehe hierzu unsere Ausführungen zu Art. 50 ff. VE-DSG).
	DSG	20	1		Wir begrüssen, dass ausdrücklich festgehalten wird, dass die Auskunft über die eigenen Personendaten (der «Zugang zu den eigenen Personendaten») als Inbegriff der Ausübung des Grundrechts auf informationelle Selbestimmung *kostenlos* zu gewähren ist.
	DSG	20	2		Wir begrüssen, dass auf Gesetzesstufe ausdrücklich festgehalten wird, welche Informationen mitgeteilt werden müssen.
	DSG	23	2	d	Es ist nicht sinnvoll, beim Profiling eine tatbestandsausschliessende Einwilligung vorzusehen. Ein Profiling im Sinne der Legaldefinition (siehe oben unseren Ergänzungsantrag zu Art. 3 lit f VE-DSG) stellt eine Persönlichkeitsverletzung dar. Sie kann aber, wie in Art. 24 Abs. 1 VE-DSG vorgesehen, durch eine Einwilligung der betroffenen Person gerechtfertigt werden – in Verbindung mit der Regelung von Art. 4 Abs. 6 VE-DSG ist klar, dass die Einbwilligung ausdrücklich erteilt werden muss. Wir beantragen deshalb, die Worte «ohne ausdrückliche Einwilligung der betroffenen Person» zu streichen.

	DSG	24	2	c	Ziff 1: Nach dem geltenden Recht waren Datenbearbeitungen durch Wirtschaftsinformationsunternehmen (Wirtschaftsauskunfteien) durch ein überwiegendes Interesse gerechtfertigt, solange diese keine Persönlichkeitsprofile bearbeiteten. Im VE-DSG wird das Persönlichkeitsprofil (als «gefährliche» Datenart) ersetzt durch das Profiling (als «gefährliche» Art der Datenbearbeitung). Im nun vorgeschlagenen Art. 24 Abs. 2 lit. c VE-DSG wird das Profiling erlaubt, ohne dass – ausser dem Erfodernis der Volljährigkeit der betroffenen Personen (Ziff. 3) – in irgendeiner Weise strengere Anforderungen an das Profiling gestellt werden. Wir beantragen, dies zu prüfen und strengere Anforderungen an das Profiling durch Wirtschaftsinformationsunternehmen zu stellen.
	DSG	25			Für betroffene Personen ist es häufig praktisch ausgeschlossen, bei Datenbearbeitungen in stark informatisierten Unternehmen die notwendigen Beweise zu erbringen, um Klagen nach Art. 25 VE-DSG (heute Art. 15 DSG) zu erbringen. Wir beantragen deshalb, bei Klagen nach Art. 25 BVE-DSG eine Beweislastumkehr vorzusehen, um die Position der betroffenen Person im Konfliktfall zu stärken.
	DSG	25			Siehe unseren Antrag zu Art. 3 lit. d VE-DSG (löschen – vernichten).
	DSG	26	1		Das Verhältnis zwischen Art. 3 lit. h und Art. 26 VE-DSG ist unklar. Nach Art. 3 lit. h VE-DSG ist das Bundesorgan verantwortlich, das, alleine oder zusammen mit anderen, über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet – nach Art. 26 Abs. 1 VE-DSG das Bundesorgan, das Personendaten bearbeitet oder bearbeiten lässt. Dieses Verhältnis ist zu klären.
	DSG	27	1		Wir entnehmen der Formulierung von Art. 27 Abs. 1 VE-DSG, dass für «gewöhnliche» Personendaten künftig beide Formen von gesetzlichen Grundlagen genügen sollen: ● *unmittelbare* gesetzliche Grundlagen, in denen ausdrücklich das *Bearbeiten* von Personendaten geregelt wird, und

					● *mittelbare* gesetzliche Grundlagen, in denen eine Aufgabe statuiert wird, die durch das zuständige Bundesorgan nur erfüllt werden kann, wenn es («gewöhnliche») Personendaten bearbeitet – mit anderen Worten: Ein Bundesorgan darf auch (aber nur «gewöhnliche») Personendaten bearbeiten, wenn dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist (für das Bearbeiten besonders schützenswerter Personendaten gelten die strengeren Voraussetzungen von Abs. 2: die Aufgabe muss in einem Gesetz im formellen Sinn geregelt sein und die Datenbearbeitung ist nur zulässlig, wenn dies zur Erfüllung der gesetzlichen Aufgabe unentbehrlich (oder wie es in kantonalen Gesetzen teilweise umschrieben ist: zwingend notwendig) ist. Wir empfehlen, dies allenfalls im Gesetzestext, mindestens aber im Botschaftstext zu klären.
	DSG	27	2		Wir weisen nochmals auf unsere Vorbemerkung betreffend Profiling (Bemerkung zu Art. 3 lit. f VE-DSG) hin: Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls. Wir beantragen zu verdeutlichen, dass aus diesem Grund ein Profiling immer eine Grundlage in einem formellen Gesetz voraussetzt (weil ein Profiling immer besondere Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen birgt und deshalb nach Art. 27 Abs. 2 lit. b VE-DSG nicht auf Grundlage einer Regeleung in einem Gesetz im materiellen Sinn zulässig ist). Zur Verdeutlichung schlagen wir vor, Satz 2 von Art. 27 Abs. 2 wie folgt zu formulieren: Eine Grundlage in einem Gesetz im materiellen Sinn ist für das Bearbeiten von besonders schützenswerten Personendaten ausreichend, wenn ...
Fehler! Verweisquelle konnte nicht gefunden	DSG	27	2	b	Wir beantragen, «die Persönlichkeit» zu streichen. Die Risiken für die Persönlichkeit bestehen v.a. beim Bearbeiten durch Private – bei den Bundesorganen sind es Risiken für die Grundrechte. Da es hier ausschliesslich um das Bearbeiten von Personendaten durch Bundesorgane geht, ist «die Persönlichkeit» zu streichen.

werden.					
	DSG	31	2		Siehe unseren Antrag zu Art. 3 lit. d VE-DSG (löschen – vernichten). Wenn hier ausschliesslich Vernichten (im Sinne der Begriffsklärung) gemeint ist, ist die Formulierung korrekt. Andernfalls müsste geprüft werden, ob es nicht heissen müsste: Sie löschen oder vernichten die ...
	DSG	34	1	a	Wir beantragen die Änderung der Formulierung: a. die widerrechtliche Bearbeitung von Personendaten unterlässt (Streichung des Wortes «betreffenden»)
	DSG	34	4		Siehe unseren Antrag zu Art. 3 lit. d VE-DSG (löschen – vernichten).
	DSG	36			Neu sollen die Bundesorgane ihre Datenbearbeitungstätigkeit melden. Nach dem Erläuternden Bericht (S. 76) entspreche diese Pflicht im Wesentlichen seiner Pflicht, eine Datensammlung anzumelden; es handle sich (bloss) um eine terminologische Anpassung infolge der Aufhebung des Begriffs der «Datensammlung» (Art. 3 Bst. g DSG). Dabei wird verkannt, dass es nicht bloss um den Ersatz des Begriffs der «Datensammlung» geht. Es ist kritisch zu hinterfragen, was das Register der Datensammlungen bis heute für den Grundrechtsschutz der betroffenen Personen geleistet hat. Wir beantragen, das Register tatsächlich auf ein *Register der Datenbearbeitungstätigkeiten* zu reduzieren – dem Sinne nach etwa so, wie es Kantone bereits bisher getan haben (vgl. z.B. § 24 IDG/BS und das Verzeichnis der Verfahren, bei denen Personendaten bearbeitet werden, unter <http://www.staatskanzlei.bs.ch/oeffentlichkeitsprinzip/verfahren.html>.
	DSG	37			Art. 37 VE-DSG spricht von Wahl und Stellung des EDÖB. Obwohl am Wahlverfahren nichts geändert wird, wird im Titel «Wahl» durch «Ernennung» ersetzt. Diese Anpassung an die europarechtliche Terminologie ist verwirrlich und entspricht nicht dem Verfahren: Wie Abs. 1 richtig festhält, wird der Beauftrage gewählt und nicht ernannt, weshalb der Titel entsprechend anzupassen ist.
	DSG	37	4		Die Budgethoheit des Beauftragten ist in Analogie zur Budgethoheit der Eidgenössischen Finanzkontrolle (EFK) gemäss Finanzkontrollgesetz (FKG; SR 614.0) auszugestalten. Der Beauftragte geniesst die gleiche

					Unabhängigkeit wie die EFK. Die Unabhängigkeit muss auch in finanzieller Hinsicht verwirklicht werden. Dazu gehört, dass der Beauftragte seinen Budgetantrag ohne direkte Intervention des Bundesrates der Bundesversammlung vorlegen kann. Entsprechend soll – analog zur EFK bzw. analog zu Art. 2 Abs. 3 FKG – der Beauftragte seinen Budgetantrag dem Bundesrat einreichen, welcher ihn unverändert an die Bundesversammlung weiterleiten muss.
	DSG	38	1		Die Möglichkeit der Wiederwahl des Beauftragten ist nicht zu beschränken. Es ist nicht ersichtlich, weshalb eine Amtszeit von mehr als 12 Jahren die Unabhängigkeit des Beauftragten schwächen soll. Auch die Richtlinie (EU) 2016/680 sowie der E-SEV 108 geben keine maximale Amtszeit vor. Die Richtlinie gibt lediglich vor, dass «die Frage, ob – und wenn ja – wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können», durch Rechtsvorschriften vorgesehen sein muss.
	DSG	39	1		Das Verbot des Beauftragten, kein Amt *eines Kantons* bekleiden zu dürfen, ist nicht notwendig. Der Beauftragte hat gegenüber den Kantonen keine Weisungsbefugnisse oder Aufsichtsfunktion in Datenschutzbelangen, weshalb besipielsweise eine ehrenamtliche Tätigkeit auf kantonaler oder kommunaler Ebene keineswegs seine Unabhängigkeit in Frage stellen würde.
	DSG	41			Es ist zu begrüssen, dass dem Beauftragten erweiterte Untersuchungsbefugnisse zugestanden werden. Dies enspricht den Vorgaben des E-SEV 108 (Art. 12^{bis} Ziff. 3) sowie der Richtlinie (EU) 2016/680 (Art. 52) entspricht. Allerdings stellen diese Vorgaben klar, dass der Beauftragte nicht die Wahl hat, ob er auf eine Anzeige einer betroffenen Person reagieren will oder nicht («kann»), da er diesbezüglich klarerweise eine Behandlungspflicht hat. Dies müsste im Gesetztestext im Verhältnis zu Art. 41 Abs. 5 besser zum Ausdruck gebracht werden. Es ist deshalb auch davon auszugehen, dass dem Beauftragte für diese Aufgabenerfüllung erheblich mehr Ressourcen zur Verfügung stehen müssen als die derzeit in den Erläuterungen erwähnten «maximal ein oder zwei Stellen». Es macht Sinn, wenn der Bundesrat die konkrete Ressourcenbenennung auf die Botschaft verschiebt, jedoch werden «maximal ein bis zwei Stellen» (vgl. Erläuternder Bericht vom 21. Dezember 2016, S. 109) auf keinen Fall reichen.

	DSG	41	5		Art. 41 Abs. 5 VE-DSG ist zu unspezifisch formuliert. Obwohl nicht davon auszugehen ist, dass dem Beauftragten eine eigentliche Untersuchungspflicht obliegt, so ist doch klarerweise von einer *Behandlungs*pflicht auszugehen. Es dürfte sich hier in Umsetzung von Art. 52 und 53 Richtlinie (EU) 2016/680 verwaltungsrechtlich wohl um eine «Aufsichtsbeschwerde» («aufsichtsrechtliche Anzeige») handeln. Entsprechend ist der Beauftragte verpflichtet, sich mit dieser Anzeige zu befassen. Art. 41 Abs. 5 VE-DSG ist verbindlicher umzuformulieren. Zusätzlich sollte noch die Behandlungsfrist von drei Monaten erwähnt werden. Zumindest müsste diesbezüglich der Botschaftstext Klarheit schaffen. Zur Ressourcenfrage vgl. die Bemerkungen zu Art. 41 VE-DSG.
	DSG	43			Gestützt auf Art. 43 VE-DSG wird dem Beauftragten lediglich die Möglichkeit von Verwaltungsmassnahmen gegeben. Allerdings verlangen die europarechtlichen Vorgaben (Art. 12^{bis} Abs. 2 lit. c E-SEV 108) wirksame, verhältnismässige und abschreckende Sanktionsmöglichkeiten. Gemäss Erläuterndem Bericht soll dies ohne Sanktionsmöglichkeiten des Beauftragten lediglich durch die erweiterten Strafbestimmungen des VE-DSG erfolgen. Der erweiterte Einbezug des Strafrechts in den Vollzug des Datenschutzrechts erscheint aber als untauglicher Weg, die europarechtlichen Vorgaben zu erfüllen (siehe hierzu unsere Ausführungen zu Art. 50 ff. VE-DSG). Der Beauftragte muss deshalb zusätzlich bei Verstössen gegen das Datenschutzrecht auch administrative Sanktionen verhängen können (etwa Bussen), und zwar mindestens gegenüber Privaten. Art. 43 VE-DSG ist entsprechend zu ergänzen.
	DSG	45			Neben der Anzeigepflicht muss in Art. 45 VE-DSG auch das Anzeigerecht statuiert werden. Das Anzeigerecht des Beauftragten bei Straftaten ergibt sich aus Art. 301 Strafprozessordnung (StPO; SR 312.0) und bezieht sich auch auf Delikte, die nicht von Amtes wegen verfolgt werden.
	DSG	49		a	Der Beauftragte hat gegenüber kantonalen Organen keine Aufsichts- oder Beratungsfunktion (vgl. dazu auch Bemerkung zu Art. 39 Abs. 1 VE-DSG). Entsprechend ist in Art. 49 lit. a VE-DSG im Verhältnis zu den kantonalen Organen die ursprüngliche Formulierung von Art. 31 lit. a DSG beizubehalten: «Er *unterstützt* Organe […] der Kantone».

	DSG	50			Vorbemerkung zu Art. 50-55 VE-DSG: Wir lehnen den Ausbau der Strafbestimmungen im VE-DSG ab. Mit den vorgesehenen Strafbestimmungen werden bisherige Vollzugsdefizite des DSG auf das Strafrecht abgewälzt. Bereits die bestehenden Strafbestimmungen des DSG haben sich in Bezug auf eine einheitliche Vollstreckung des DSG nicht bewährt. Strafurteile aufgrund der Strafbestimmungen des DSG sind fast gänzlich unbekannt. Mi den neuen Bestimmungen tritt der Strafrichter in Konkurrenz zur Datenschutzaufsichtsbehörde, was weder institutionell noch sachlich sinnvoll ist. Zahlreichen der neuen Strafbestimmungen fehlt die Bestimmtheit, so dass sie dem Grundsatz «Nulla poenae sine lege» widersprechen (siehe Bemerkungen zu Art. 51 und 51 VE-DSG). Mit den umschriebenen Strafbestimmungen werden die Vorgaben gemäss Richtlinie (EU) 2016/680 und Art. 12^{bis} Abs. 2 Bst. c E-SEV 108 nicht vollständig umgesetzt. Die EU sowie der Europarat verlangen ausdrücklich auch Verwaltungssanktionen, die der Beauftragte verhängen kann (vgl. dazu auch die Bemerkungen zu Art. 45 VE-DSG). Die angedrohten strafrechtlichen Sanktionen von max.500 000 CHF wirken keinesfalls abschreckend und sind im Vergleich zu den Sanktionsmöglichkeiten nach dem EU Recht für global tätige Unternehmen bedeutungslos. Mit den Strafbestimmungen wird die Strafverfolgung zudem an die Kantone delegiert. Damit müssen die Kantone nicht nur ressourcenmässig für den Vollzug des VE-DSG aufkommen, sondern es ist aufgrund der spezifischen Materie des Datenschutzrechts auch damit zu rechnen, dass kein einheitlicher Vollzug möglich sein wird. Der Vollzug und die Sanktionierung von Verstössen gegen das VE-DSG sind aus unserer Sicht eine Bundesaufgabe und somit durch den Bund wahrzunehmen (vgl. auch Bemerkung zu Art. 54 VE-DSG). Daraus ergibt sich, dass die Sanktionsmöglichkeiten des Beauftragten auszubauen sind (siehe Bemerkungen zu Art. 43 VE-DSG) und die Organisation allenfalls analog der Wettbewerbskommission

					auszubauen ist (vgl. Erläuternder Bericht. S. 83). Die Kompetenz zur Sanktionierung liegt damit beim Beauftragten, weshalb die Strafbestimmungen entsprechend umzufomulieren sind.
	DSG	50			Wir stellen fest, dass die maximale Busse von 500 000 CHF respektive 250 000 CHF bei Fahrlässigkeit nicht abschreckend zu wirken vermag und deshalb entsprechend zu erhöhen ist. Zum Vergleich: In der EU sind Bussen bis zu 20 000 000 Euro resp. bei Unternehmen bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres möglich, wobei der höhere Betrag massgeblich ist (vgl. Art. 83 Abs. 5 Verordnung (EU) 2016/679). Vgl. auch die Bemerkungen zu Art. 53 VE-DSG betreffend Übertretungen in Geschäftsbetrieben.
	DSG	50	1,2,3		Der Norm fehlt es weitgehend an der Bestimmtheit, und damit ist auch die Möglichkeit der Strafbarkeit nicht gegeben. Als Beispiel sei die Informationspflicht gemäss Art. 15 VE-DSG erwähnt, die besteht, wenn eine Datenbearbeitung «erhebliche Auswirkungen» auf die betroffene Person hat. «Erhebliche Auswirkungen» dürfte wohl kaum als objektives Tatbestandsmerkmal vor den strafrechtlichen Kriterien standhalten.
	DSG	51			Wie bei Art. 50 VE-DSG fehlt es auch hier an der Bestimmtheit der Norm.
	DSG	52			Mit Art. 52 VE-DSG soll der in Art. 321 Strafgesetzbuch (StGB; SR 311.0) festgehaltene Schutz beruflicher Schweigepflichten vervollständigt werden (Erläuternder Bericht, S. 85). Dieser Zweck wird mit dieser Bestimmung jedoch nicht erreicht. Es stellt sich insbesondere die Frage, was «geheime» Personendaten sind (Korrelation mit Art. 321 StGB wird nur durch die Erläuterungen ersichtlich). Zudem stellt sich die Frage, wer als Täter konkret in Frage kommt: Jeder Mitarbeiter eines Unternehmens? Auch Mitarbeiter der Bundesverwaltung? In welchem Verhältnis dazu steht dann das Amtsgeheimnis gemäss Art. 320 StGB? Der Zweck dieser Bestimmung ist zu überprüfen und die Formulierung in Bezug auf das strafrechtliche Bestimmtheitsgebot neu zu fassen.
	DSG	53			Da strafrechtlichen Ermittlungen gegen eine Person in einem Unternehmen schwierig sind, ist es zu begrüssen, dass der Geschäftsbetrieb sanktioniert werden kann. Allerdings gbit es keinen Grund, die

					maximal Bussenhöhe zu reduzieren.
	DSG	54			Mit dieser Bestimmung wird die Sanktionierung von Verstössen gegen das Datenschutzgesetz an die Kantone delegiert (vgl. dazu auch die Vorbemerkungen zu Art. 50-55 VE-DSG. Damit müssen die Kantone nicht nur ressourcenmässig für den Vollzug des VE-DSG aufkommen, sondern es ist aufgrund der spezifischen Materie des Datenschutzrechts auch damit zu rechnen, dass kein einheitlicher Vollzug möglich sein wird. Der Vollzug und die Sanktionierung von Verstössen gegen das VE-DSG sind aus unserer Sicht eine Bundesaufgabe und somit durch den Bund wahrzunehmen.
	DSG	57			Dieser Artikel ist zu streichen. Seit dem Beitritt der Schweiz zum Schengenraum (Schengener-Assoziierungsabkommen) resp. spätestens mit der Umsetzung der neuen Richtlinie (EU) 2016/680 und bei Ratifizierung des revidierten Übereinkommens SEV 108 sind auch die Kantone verpflichtet, einen angemessenen Schutz von Personendaten durch unabhängige Datenschutzaufsichtsbehörden zu gewährleisten. Diese «Auffangnorm» ist daher obsolet und kann gestrichen werden.
	DSG	Anh.	Ziff. 5		BGÖ (SR 152.3): Art. 9 Ergänzung: In Art. 9 Abs. 2 BGÖ ist der Verweis auf das DSG ebenfalls anzupassen: neu Art. 29 Datenschutzgesetz (anstelle von Art. 19 Datenschutzgesetz).
	DSG	Anh.	Ziff. 10		Bundesgesetz vom 24.3.2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten (SR 235.2): Art. 1 zweiter Satz: Vgl. unsere Bemerkungen zu Art. 3 lit. f und Art. 27 Abs. 2 VE-DSG: Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls. Wir beantragen, dem Profiling hier hinreichend bestimmt Grenzen zu setzen.

	DSG	Anh.	Ziff. 11		ZPO (SR 272): Die ZPO soll dahingehend geändert werden, dass für Klagen und Begehren nach dem Datenschutzgesetz keine Sicherheiten zu leisten und keine Gerichtskosten zu bezahlen sind. Diese Erleichterungen in der Prozessführung für die betroffene Person können für sich die Schwelle für die Durchsetzung der eigenen Rechte nicht herabsetzen. Die in den Erläuterungen aufgrund des Fehlens von wirkungsvollen Rechtsdurchsetzungsinstrumenten vor allem im privaten Sektor festgestellte erheblich verringerte Wirksamkeit des Datenschutzgesetzes kann nur aufgefangen werden, wenn neben der Kosten auch die Beweisführung für die betroffene Person erleichtert wird. Wir empfehlen deshalb für Verfahren aufgrund des Datenschutzgesetzes eine Beweislastumkehr, da es der betroffenen Person aufgrund der Komplexität der heutigen Datenbearbeitungen gar nicht möglich ist, den Beweis für das unbefugte Bearbeiten zu erbringen. Dies bedeutet auch keine zusätzliche Belastung des Verantwortlichen, da dieser den Nachweis der Konformität seiner Datenbearbeitungen auch unabhängig von einem Verfahren zu dokumentieren hat (Art. 19 lit. a VE-DSG).
	DSG	Anh.	Ziff. 16		BPI (SR 361), Art. 3 Abs. 2: Vgl. unsere Bemerkungen zu Art. 3 lit. f und Art. 27 Abs. 2 VE-DSG: Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls. Wir beantragen, dem Profiling hier hinreichend bestimmt Grenzen zu setzen.
	DSG	Anh.	Ziff. 25		MIG (SR 510.91), Art. 1 Abs. 1 Einleitungssatz: Vgl. unsere Bemerkungen zu Art. 3 lit. f und Art. 27 Abs. 2 VE-DSG: Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls. Wir beantragen, dem Profiling hier hinreichend bestimmt Grenzen zu

					setzen.
	DSG	Anh.	Ziff. 28		BZG (SR 520.10), Art. 72 Abs. 1 und 1bis: Vgl. unsere Bemerkungen zu Art. 3 lit. f und Art. 27 Abs. 2 VE-DSG: Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls. Wir beantragen, dem Profiling hier hinreichend bestimmt Grenzen zu setzen.
	DSG	Anh.	Ziff. 35		LFG (SR 748.0), Art. 107a Abs. 2: Vgl. unsere Bemerkungen zu Art. 3 lit. f und Art. 27 Abs. 2 VE-DSG: Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls. Wir beantragen, dem Profiling hier hinreichend bestimmt Grenzen zu setzen.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung

Dachverband
gemeinnütziger
Stiftungen
der Schweiz

Dufourstrasse 49
CH-4052 Basel
Schweiz

Telefon ++41 61 272 10 80
Telefax ++41 61 272 10 81
www.profonds.org

Nur per E-Mail an: jonas.amstutz@bj.admin.ch

Frau Bundesrätin
Simonetta Sommaruga
Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Basel, 04. April 2017 CDE/RBA/vje

Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG)

Sehr geehrte Frau Bundesrätin

proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz, vertritt gesamtschweizerisch die Interessen *gemeinnütziger Stiftungen und Vereine* aller Tätigkeits- und Finanzierungsformen. Dem Gemeinnützigkeitswesen kommt in der Schweiz sehr grosse Bedeutung zu. Die rund 13'000 gemeinnützigen Stiftungen und die zahlreichen gemeinnützigen Vereine üben im Interesse und zum Wohl der Allgemeinheit wichtige Funktionen aus, etwa in den Bereichen Soziales, Gesundheitswesen, Forschung und Wissenschaft, Bildung und Erziehung, Jugendförderung, Kunst, Kultur, Entwicklungszusammenarbeit etc.

Gerne machen wir von der Möglichkeit Gebrauch, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes eine Vernehmlassung einzureichen. Wir haben den Vorentwurf unseren rund 430 Mitgliedern zur Stellungnahme unterbreitet. Die Rückmeldungen aus dieser *internen Konsultation* fanden Eingang in die vorliegende Vernehmlassung.

Vorbemerkung

Zahlreiche gemeinnützige Stiftungen und Vereine werden vom totalrevidierten Datenschutzgesetz betroffen sein. Im Vordergrund stehen namentlich Aktivitäten im Zusammenhang mit dem Fundraising (Spenderdaten) und – für Vereine – den Mitgliederdaten. In diesen Bereichen werden Personendaten bearbeitet.

Beim Gros der gemeinnützigen Stiftungen und Vereine handelt es sich um kleinere und mittlere Organisationen ohne nennenswerte Personalressourcen. Nach wie vor ist die Ehrenamtlichkeit, d. h. unentgeltliches Engagement, weit verbreitet,

namentlich in den Leitungsgremien (Stiftungsrat und Vereinsvorstand). Das Gros der gemeinnützigen Stiftungen und Vereine verfügt auch über sehr begrenzte finanzielle Mittel. Zudem setzen die sehr tiefen Zinsen und starken Volatilitäten der Börsen den gemeinnützigen Organisationen stark zu.

Die Anwendung des geplanten neuen Datenschutzgesetzes wird zahlreiche gemeinnützige Stiftungen und Vereine überfordern. Der komplexe Gesetzesentwurf wird die Stiftungen und Vereine zwingen, das erforderliche Know-how extern einzukaufen. Dies wird die finanziellen Ressourcen unangemessen strapazieren, wenn nicht gar übersteigen und dazu führen, dass weniger Mittel für die Erfüllung des gemeinnützigen Zwecks zur Verfügung stehen. Wir bedauern dies und erkennen darin eine weitere Überregulierung, die den Schweizer Gemeinnützigkeitsstandort benachteiligen wird.

proFonds vertritt die Auffassung, dass das bestehende Datenschutzgesetz genügt. Dessen Umsetzung ist wesentlich effizienter und kostengünstiger, als es beim neuen Gesetz der Fall wäre.

proFonds hat ein gewisses Verständnis dafür, dass die Schweiz das revidierte europäische Recht (Übereinkommen SEV 108; EU-Datenschutzgrundverordnung) nachvollziehen will, ist aber strikt dagegen, über die Anforderungen der EU hinauszugehen. Ein solcher *Swiss Finish* ist nicht nur unnötig, sondern mit einem liberalen, standortfreundlichen Verständnis und dem Gebot der Praktikabilität – gerade auch in ehrenamtlichen bzw. Miliz-Strukturen – nicht zu vereinbaren.

Es darf nicht sein, dass das freiwillige Engagement von Bürgerinnen und Bürgern zum Wohl der Gesellschaft in ein noch engeres gesetzliches Korsett gedrängt wird. Der vorliegende Gesetzesentwurf würde dies tun und geht damit in die falsche Richtung.

Zu einzelnen gesetzlichen Regelungen

Profiling (Art. 3 lit. f. E-DSG)

Der Begriff Profiling ist äusserst breit und geht über die Anforderungen der EU-Regelung hinaus. Ein Profiling soll überdies ohne ausdrückliche Einwilligung der betroffenen Personen *per se* persönlichkeitsverletzend sein (vgl. Art. 23 Abs. 2 lit. d E-DSG).

Letztere Regelung halten wir für massiv übertrieben und **beantragen** entsprechend eine ersatzlose Streichung. Der Begriff Profiling ist demgegenüber angemessen einzuschränken.

Bekanntgabe ins Ausland (Art. 5 f. E-DSG)

Die Bekanntgabe von Daten ins Ausland wird unnötigerweise erschwert. Es ist damit zu rechnen, dass die Bekanntgabe aufgrund der gesetzlichen Pflichten komplizierter und langwieriger wird. Insbesondere drohen empfindliche Sanktionen bei Verletzung der Pflichten von Art. 5 E-DSG (vgl. dazu hinten zu den Strafbestimmungen).

Datenschutz-Folgenabschätzung (Art. 16 E-DSG)

Das neue Instrument der Datenschutz-Folgenabschätzung ist problematisch. Es wird namentlich kleine und mittlere Stiftungen und Vereine überfordern. Zudem wäre mit erheblichen Kosten zu rechnen, um die Folgenabschätzung umzusetzen.

Der Anwendungsbereich der Datenschutz-Folgenabschätzung ist spürbar einzugrenzen. Sie soll nach dem Wortlaut des Entwurfs bereits bei einem *"erhöhten Risiko"* für die Persönlichkeit der betroffenen Person zur Anwendung gelangen. Wann ein solches erhöhtes Risiko vorliegt, ist unklar. Es ist damit zu rechnen, dass dies in der Praxis rasch angenommen wird. Demgegenüber verlangt die EU für die Durchführung einer Folgenabschätzung ein "hohes Risiko".

Der für die gemeinnützigen Stiftungen und Vereine erforderliche administrative Aufwand für die Durchführung einer Folgenabschätzung wäre enorm. Er stünde in keinem Verhältnis zum Nutzen der Folgenabschätzung.

proFonds **beantragt**, den Anwendungsbereich der Datenschutz-Folgenabschätzung deutlich einzuschränken. Allenfalls wäre sogar eine Ausnahme davon für gemeinnützige Organisationen zu prüfen.

Meldung von Verletzungen des Datenschutzes (Art. 17 E-DSG)

Der Entwurf sieht vor, eine Meldepflicht für diejenigen Datenbearbeitungen einzuführen, die gegen den Datenschutz verstossen. Dies ist nicht nur übertrieben, sondern geht erneut über dasjenige hinaus, was die EU verlangt.

Solche Datenschutzverletzungen dürften in der Praxis häufig vorkommen. Eine Meldepflicht ist unangebracht, namentlich unter dem Aspekt der scharfen Strafdrohung bei Verletzung der Meldepflicht (vgl. Art. 50 Abs. 2 lit. e E-DSG).

proFonds **beantragt** eine *Reduktion der Meldepflicht auf ein vernünftiges Mass*, mindestens auf das Niveau der EU. In der EU ist eine Meldung nur dann erforderlich, wenn festgestellt wird, dass eine getroffene Sicherheitsmassnahme verletzt wurde und diese Verletzung zu einem Bruch oder Verlust des Datengewahrsams führt.

Weitere Pflichten (Art. 19 Abs. 1 lit. a E-DSG)

proFonds bezweifelt die Notwendigkeit der Pflicht, alle Datenbearbeitungen zu dokumentieren. Die Bestimmung ist zudem bezüglich Inhalt und Umfang unklar. Sie geht über die vergleichbaren Bestimmungen der EU hinaus. Wird diese Pflicht nicht sachgerecht eingeschränkt, ist in der Praxis gerade bei kleinen und mittleren Stiftungen und Vereinen mit beträchtlichem Mehraufwand zu rechnen.

proFonds **beantragt** eine sinnvolle sachliche Begrenzung dieser Pflicht.

Strafbestimmungen (Art. 50 ff. E-DSG)

Das geltende DSG kennt von der Übertretungsnorm gemäss Art. 34 DSG abgesehen keine nennenswerten Strafbestimmungen. Dieser Zustand soll nun durch Einführung scharfer Sanktionen geändert werden.

Die neuen Strafbestimmungen von Art. 50 ff. E-DSG richten sich gegen private Personen, bei Vereinen und Stiftungen in der Regel also gegen Organe und Mit-

arbeiter. Erfasst werden auch fahrlässige Datenschutzverstösse, was zu einer stossenden Kriminalisierung von Organen und Mitarbeitern führen wird. Die Bussenobergrenze von CHF 500'000 (für vorsätzliche Tatbegehung) und CHF 250'000 (für fahrlässige Tatbegehung) ist massiv und unverhältnismässig.

Die flächendeckende Kriminalisierung dürfte dazu führen, dass sich Organe und Mitarbeiter davor hüten werden, ohne externe Beratung Entscheide im Bereich der Datenbearbeitung zu treffen. Dies führt wiederum zu einem Kostenschub mit dem Ergebnis, dass die dadurch absorbierten Stiftungs- oder Vereinsmittel nicht mehr für die Erfüllung des gemeinnützigen Zwecks zur Verfügung stehen.

proFonds **beantragt**, die Strafbestimmungen in dem Sinn zu überarbeiten, dass sie hinsichtlich Anwendungsbereich und Sanktionshöhe auf ein vernünftiges Mass reduziert werden. Die Fahrlässigkeitsdelikte sind ersatzlos zu streichen.

Art. 52 E-DSG führt schliesslich eine neue berufliche Schweigepflicht ein, deren Missachtung mit Freiheitsstrafe bis zu drei Jahren pönalisiert ist. Jeder Berufstätige untersteht damit einer sanktionierten Schweigepflicht und zwar unabhängig davon, ob die Daten selbst einer Geheimhaltung unterliegen. Diese Regelung ist übertrieben.

proFonds **beantragt**, Art. 52 E-DSG vollständig zu entfernen und die bisherige Regelung von Art. 35 DSG zu belassen.

Wir danken Ihnen für die aufmerksame Prüfung unserer Standpunkte und Anträge. Wir hoffen, dass diese bei der weiteren Bearbeitung der Vorlage Berücksichtigung finden. Für eine Vertiefung spezifischer Fragen steht proFonds jederzeit gerne zur Verfügung.

Mit freundlichen Grüssen

François Geinoz
Präsident

Dr. Christoph Degen
Geschäftsführer

Amstutz Jonas BJ

Von: info@promoswiss.ch
Gesendet: Montag, 3. April 2017 14:27
An: Amstutz Jonas BJ
Cc: 'Racol Partner AG'; 'KS-Sekretariat'
Betreff: Vernehmlassungsverfahren: Datenschutzgesetz
Anlagen: Stellungnahme DSG Revision 2017.doc

Guten Tag Herr Amstutz

Anbei senden wir Ihnen die Stellungnahme des PROMO SWISS VERBANDES zur Totalrevision des Datenschutzgesetzes.

Freundliche Grüsse

Adrian Schmidhäusler

PROMOSWISS Verband
Verband der Schweizerischen Werbeartikelindustrie
Sekretariat, Postfach 429, 8853 Lachen
Mob. ++41 (0)79-710 22 69
http://www.promoswiss.ch
mail: info@promoswiss.ch

PROMO SWISS
Verband der Schweizerischen Werbeartikelindustrie
Association professionnelle Suisse pour la publicité par l'objet
Associazione Svizzera di professionisti per l'articolo pubblicitario

Stellungsnahme von PROMOSWISS zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

PROMOSWISS ist der Verband der Schweizerischen Werbeartikelindustrie und steht im Dienst der in der Schweiz ansässigen Werbeartikel-Handelsfirmen und der Werbeartikel-Hersteller. Die Werbeartikelbranche erwirtschaftet in der Schweiz etwa 700 Mio Franken, umfasst etwas mehr als 300 Betriebe und beschäftigt rund 1'750 Personen. Viele dieser Betriebe sind kleinere Unternehmungen.

Gerade für diese Klein- und Kleinstunternehmen ist es von entscheidender Bedeutung, dass die staatlichen Regulierungen, Gesetze und Bestimmungen nicht strenger ausgelegt werden, als im benachbarten Ausland. Dies ist mit dem jetzt vorgelegten Entwurf des Datenschutzgesetzes leider nicht gegeben. Etliche Positionen werden gegenüber dem Europäischen Pendant schärfer gefasst und bedrohlich ausgeweitet. Diese Verschärfungen lehnen wir vollumfänglich ab.

Einige Artikel des DSG (19/23/24/50ff/52) sind für die von uns vertretenen Betriebe existentiell bedrohend. Sowohl die Werbeartikel wie auch unsere Kommunikation werden oft personalisiert eingesetzt. Das neue DSG würde zu einem grossen Standortnachteil für die Schweizerischen Handelsfirmen führen. Ein Grossteil unserer KMU-Firmen wäre sowohl finanziell als auch personell überfordert, die Umsetzung des neuen DSG hätte für unsere Branche schwerwiegende Folgen.

Wir erinnern gerne daran, dass genau die von uns vertretenen KMUs das Rückgrat der Schweizer Wirtschaft bilden.

Im Weiteren und in Detailfragen verweisen wir auf die ausführliche Stellungnahme des Schweizerischen Dialogmarketing Verbandes (SDV) und von Kommunikation Schweiz (KS/CS).

PROMOSWISS bedankt sich im Voraus für die Berücksichtigung der Anliegen und freut sich auf eine verhältnismässige und wirtschaftstaugliche Umsetzung der Totalrevision des Datenschutzgesetzes.

Mit freundlichen Grüssen

PROMOSWISS
Verband der Schweizerischen Werbeartikelindustrie

Roger Riwar	Adrian Schmidhäusler
Präsident	Geschäftsführer

Amstutz Jonas BJ

Von: tenzin.kartso@swisseshop.ch
Gesendet: Dienstag, 4. April 2017 12:05
An: Amstutz Jonas BJ
Betreff: Stellungnahme zum DSG-Entwurf
Anlagen: PROTARIS-Stellungnahme_de_VE-DSG.doc

Guten Tag Herr Amstutz

Unsere Bedenken betr. neuem DSG-Entwurf entnehmen Sie dem Formular im Anhang.

Freundliche Grüsse

Tenzin Kartso

Tenzin Kartso
Protaris AG
Schachenstrasse 82
8645 Rapperswil – Jona

Website: www.swisseshop.ch
E-Mail: tenzin.kartso@swisseshop.ch

-----Ursprüngliche Nachricht-----
Von: Richard Lins [mailto:rli@ftargeting.ch]
Gesendet: Dienstag, 4. April 2017 12:02
An: 'Tenzin Kartso (tenzin.kartso@swisseshop.ch)' <tenzin.kartso@swisseshop.ch>
Betreff: AW: Stellungnahme zum DSG-Entwurf

Von: Richard Lins
Gesendet: Dienstag, 4. April 2017 11:57
An: 'Tenzin Kartso (tenzin.kartso@swisseshop.ch)' <tenzin.kartso@swisseshop.ch>
Betreff: AW: Stellungnahme zum DSG-Entwurf

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Protaris AG

Abkürzung der Firma / Organisation : swisseshop.ch

Adresse : Schachenstrasse 82, 8645 Jona

Kontaktperson : Tenzin Kartso

Telefon : 043 544 08 30

E-Mail : rli@ftargeting.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
swisseshop.ch	Wir verlangen gleiche Rechte wie die Amerikaner im Datenschutz. Es kann nicht sein, dass der Konsumentenschutz eine Zuskunfsbranche zum Erliegen bringt.
swisseshop.ch	Wir wissen nicht wie wir in unserem kompetetiven Online-Markt die höheren Kosten stemmen sollen, die durch die Verschärfung des Datenschutzes auf uns zu kommen.
swisseshop.ch	Wir sind ein zu kleiner Onlineshop, um extra einen Datenschutzbeauftragten einzustellen. Wir wissen nicht, wie wir die Anwaltskosten für die Umsetzung des neuen DSG bezahlen sollen.
swisseshop.ch	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
swisseshop.ch	DSG	50			Strafverfolgung von Privaten macht überhaupt kein Sinn.
swisseshop.ch	DSG	16			Das Gesetz muss betr. Datenschutzfolgeabschätzung drastisch minimiert werden.
swisseshop.ch	DSG	19			Bei der Dokumentationspflicht muss zwischen Gross- & Kleinbetrieben unterschieden werden. Der administrative Aufwand wird ansonsten viele kleine Firmen killen.
swisseshop.ch	DSG	20			Wir sehen keinen Grund das bisherige bewährte Auskunfsrecht zu ändern.
swisseshop.ch	DSG	7			Wir sehen keinen Grund die bisherige Praxis bei der Auftragsdatenbearbeitung zu ändern.
swisseshop.ch					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
swisseshop.ch	
swisseshop.ch	
swisseshop.ch	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
swisseshop.ch	
swisseshop.ch	
swisseshop.ch	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
swisseshop.ch		
swisseshop.ch		
swisseshop.ch		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
swisseshop.ch		
swisseshop.ch		
swisseshop.ch		

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

(vorab per Email in Word- und PDF-Fassung an: jonas.amstutz@bj.admin.ch)

Nidau, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt Quickline AG gerne wahr.

Quickline AG ist eine Anbieterin von Telekommunikationsnetzinfrastrukturen und -dienstleistungen mit über 400‘000 Kunden in der Schweiz. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung

zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung“ durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur“ sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish“

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale

Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung

der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-Shop“ nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden.“). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands.“[2]

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen.“[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die an-

[1] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

[2] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

[3] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

wesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichenden Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2017 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80'000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365" für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

> sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei.“[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40‘000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10‘000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5‘000 – 10‘000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5‘000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7‘500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5‘000 – 30‘000
Privacy by Default	1 – 40 Stunden		500 – 5‘000
Betriebliche Datenschutzbeauftragter		500 – 2‘000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5‘000

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1‘532‘160‘000, resp. im Durchschnitt von CHF 2‘520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die

[6] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

[7] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

[8] In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14‘000 – 149‘000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

[9] 608‘000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

> Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen.“[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

[10] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (<u>neu</u>)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*“ grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (<u>Beispiel</u>: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz“, Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis“ abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die <u>zum Zweck</u> der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten“. Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten“. Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten“ konsumiert. Der Begriff des „Profiling“ ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil“ des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling“ gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish“ versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage“ eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling“ verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist“ gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag“ (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag“ wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter“).
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten“ aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit“ einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig“, „freiwillig und eindeutig“, „ausdrücklich“ und die Abgrenzung zur blossen „Einwilligung“ (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig“, „eindeutig“ oder „ausdrücklich“ auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise“ völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen. [5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste. **Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen. **Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen“ Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche“ Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen“ reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish“ erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant“ zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves“ und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4.	
[3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten“ und „Persönlichkeitsprofilen“. Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat“. Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet; b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist; d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. **Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert. **Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. [3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle [1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. [2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen [1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. [2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. [3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1“ (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen. [2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen“. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen“ und ersetzen mit „seine Untersuchungen“. Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500‘000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1‘000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5‘000 – 30‘000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten“ wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom … *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom…. *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom ……	
Art. 114 Bst. f Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …….	
Art. 243 Abs. 2 Bst. d [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 … Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Nicolas Perrenoud
CEO

Frédéric Goetschmann
CFO

Amstutz Jonas BJ

Von: Urs Krapf <urs.krapf@raiffeisen.ch>
Gesendet: Dienstag, 4. April 2017 09:23
An: Amstutz Jonas BJ
Cc: Nadja Ceregato; Christian Bopp; Christian Bentz
Betreff: Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)
Anlagen: 20170404_VE-DSG_Stellungnahme EJPD_Final (0769564).doc
Signiert von: urs.krapf@raiffeisen.ch

Sehr geehrter Herr Amstutz

Im Dezember 2016 haben Sie uns eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetztes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. Raiffeisen nimmt im beiliegenden Dokument entsprechend Stellung zum VE-DSG.

Allfällige Fragen beantworte ich Ihnen gerne.

Freundliche Grüsse

Urs Krapf

_____

Urs Krapf
Compliance Officer

Raiffeisen Schweiz
Genossenschaft
Raiffeisenplatz
9001 St.Gallen

Telefon 071 225 84 94
Fax 071 225 88 05
www.raiffeisen.ch
urs.krapf@raiffeisen.ch
Direktwahl 071 225 95 72

_____

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Raiffeisen Schweiz

Abkürzung der Firma / Organisation : RCH

Adresse : Raiffeisenplatz 4, Postfach, 9001 St. Gallen

Kontaktperson : Urs Krapf / Christian Bentz

Telefon : 071 225 95 72 / 071 225 81 43

E-Mail : urs.krapf@raiffeisen.ch / christian.bentz@raiffeisen.ch

Datum : 04.04.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
RCH	Das DSG konkretisiert das in Artikel 13 Absatz 2 BV festgehaltene Recht auf informelle Selbstbestimmung mit Personendaten, d. h. das Recht einer Person selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen. Das derzeit gültige Datenschutzgesetz stammt aus dem Jahre 1992. Der Datenschutz in der Schweiz soll gestärkt, an internationale Standards und an die Moderne angepasst werden. Die vorgeschlagenen Änderungen im Vernehmlassungsentwurf begrüssen wir, sofern diese zu einer effektiven Verbesserung des Datenschutzes für die betroffene Person resp. zu einer Modernisierung führen, aber stets unter stringenter Berücksichtigung von Kostenaspekten für deren Umsetzung und soweit den Grundsätzen der Praktikabilität Rechnung getragen wird. Nur so kann sichergestellt werden, dass die Interessen der betroffenen Personen und der Unternehmungen in einem austarierten Verhältnis stehen und der Grundsatz der Verhältnismässigkeit eingehalten ist. Generell erheben wir die nachstehenden Einwände:
RCH	Bestehende Konzepte und Begrifflichkeiten sind weggefallen, insbesondere die Rolle des Datenschutzbeauftragten und der Begriff der „Datensammlung“. Dies führt bei Unternehmen zu Unklarheiten in der Zuweisung von Aufgaben, Kompetenzen, Verantwortlichkeiten an eine oder mehrere Personen in der Umsetzung der Bestimmungen des DSG und zu Auslegungsschwierigkeiten bei der Zuordnung von Daten, welche unter das DSG fallen bzw. nicht darunter fallen.
RCH	Um internationalen Standards gerecht zu werden, bedarf es keiner Gesetzesreform in diesem Umfang. Teilweise enthält der Entwurf Bestimmungen, welche über die Anforderungen der europäischen DSGVO hinausgehen („Swiss Finish“). Nach dem Rechtsverständnis der EU steht der Konsumentenschutz im Vordergrund, welchem die europäische DSGVO Rechnung trägt. Mit dem DSG erfolgt in Teilen nicht nur eine Angleichung an europäische Standards und eine Erweiterung des Konsumentenschutzes, sondern es erfolgt eine darüberhinausgehende Regelung. Dies ist zu vermeiden.
RCH	Die EU fordert von der Schweiz eine „dynamische Rechtsübernahme“. Das Schweizer Rechtsverständnis ist bei der Rechtssetzung vom Grundsatz der Verhältnismässigkeit geprägt resp. prinzipienbasiert. Eine unkritische Übernahme von EU-Recht lehnen wir ab. Beispielsweise wurden ohne Abwägung der Konsequenzen die Konzepte „Privacy by Design“ und „Privacy by Default“ in das neue DSG aufgenommen. Durch die neu vorgesehenen strengen Datenschutzvorgaben werden Unternehmen dazu angehalten, bereits in der Planungsphase (neue Datensammlung, neue elektronische Kanäle, Evaluation neuer Systeme etc.) den Datenschutz als Grundeinstellung in ihrem Angebot zu verankern. Dies bedeutet einen sehr ho-

	hen, kostspieligen Umsetzungsaufwand für die Unternehmen unter Missachtung des Grundsatzes der Verhältnismässigkeit durch den Gesetzgeber. Um die in der Regulierungsfolgenabschätzung (RFA) genannten erhöhten Kosten bzw. die Zunahme des Bearbeitungs- und Administrationsaufwands für Unternehmen begrenzen zu können, sind die geplanten Handlungspflichten und Massnahmen auf den Grundsatz der Verhältnismässigkeit hin zu überprüfen. Raiffeisen rechnet mit einem substanziellen Aufwand und teilt in diesem Punkt die Aussagen in der Regulierungsabschätzung.
RCH	Teilweise greifen die Bestimmungen stark in die unternehmerischen Freiheiten ein und sind in der Praxis nicht umsetzbar. Dies führt zu unerwünschten Rechtsunsicherheiten.
RCH	Eine Überbindung zahlreicher Pflichten und die damit verbundene Pönalisierung der Unternehmen resp. der für sie handelnden natürlichen Personen führen selbst bei fahrlässigen Bagatellfällen zu einer Kriminalisierung der involvierten Personen, was zu vermeiden ist.
RCH	Die europäische DSGVO ist inkonsistent eingebunden. Die inhaltliche Abstimmung bezüglich Übernahme von Bestimmungen der DSGVO in das DSG erfolgt nicht in genügendem Masse. Dies ist jedoch unabdingbar, damit ein gleichwertiger Datenschutz im Verhältnis zu anderen Staaten bestehen bleibt.
RCH	Es werden unterschiedliche Begrifflichkeiten in der französischen und der deutschen Version verwendet. Bei einer solch weitreichenden Gesetzgebung ist eine sorgfältige Abstimmung zwingend.
RCH	Den Auftragsbearbeitern werden zahlreiche verschärfte Prüf- und Meldepflichten überbunden. Das Gesamtpaket dieser Pflichten mag für spezifische Marketing-Dienstleistung und Data-Miner angemessen sein, da sie typischerweise besonders sensible Datenbearbeitungen vornehmen. Für Auftragsdatenbearbeiter, welche ständig und in hohen Volumen Daten im Zusammenhang mit der Ausführung von Kundenaufträgen und aufgrund regulatorischer Vorgaben an zahllose Empfänger weitergeben müssen, ist die pauschale Anwendung solcher Regeln unbesehen der Sensibilität der betroffenen Daten nicht sachgerecht. Sie führen nicht zu einem besseren Datenschutz, sondern lediglich zu unnötigem Aufwand und zu einer Flut von Meldungen an den Beauftragten.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
RCH	DSG	3			Die zentralen Begriffe „Personendaten“ und „Daten“ verwendet das DSG nicht konsistent. Dies führt in der praktischen Anwendung der Bestimmungen des DSG zu Rechtsunsicherheit bzw. Auslegungsschwierigkeiten.
RCH	DSG	3		a	Die Umschreibung des Begriffs „Personendaten“ ist formell unverändert geblieben. Der Wegfall des Begriffs „Datensammlung“ erschwert in der Praxis die Einordnung von Personendaten. Wir nehmen an, es handelt sich hier um ein redaktionelles Versehen. Damit einher geht die Frage, wann einzelne Daten durch Herstellung von Verbindungen, Profilierungen usw. zu Personendaten i. S. des DSG werden. Dies führt zwangsläufig zu Abgrenzungsschwierigkeiten und verursacht Rechtsunsicherheit. Der letzte Absatz des Erläuterungsberichtes führt zu mehr Verwirrung als Klärung: *„Ist darüber hinaus von Daten die Rede, handelt es sich um Daten, die keine Personendaten sind, wie dies beispielsweise beim Profiling der Fall ist.“* Wir verstehen anhand dieser Ausführungen nicht, welche konkreten Daten beim Profiling ausgenommen sind.
RCH	DSG	3		d	Eine vollständige Löschung/Vernichtung von Personendaten ist aufgrund von technischen Restriktionen nur mit erheblichem Aufwand umsetzbar. Eine Standardsoftware unterstützt nicht das vollständige Löschen von Kundendaten, sondern lediglich deren Inaktivierung zwecks Sicherstellung einer konformen Historisierung. Die Anforderung muss lauten, dass die Daten nicht mehr angezeigt oder weitergeleitet werden können. Ein Zugriff auf die Daten ist lediglich in Sonderfällen (z. B. bei Rechtsanfragen) mit Sonderrechten gemäss neuem DSG möglich. Wir schlagen folgende Formulierung vor: „Bearbeiten: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren,

					insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, ~~Löschen oder Vernichten~~ **Unzugänglich machen** von Daten;“
RCH	DSG	3		f	Die Definition des Profiling im DSG geht über die Vorgaben der europäischen DSGVO (vgl. Artikel 4, Ziffer 4) hinaus und stellt einen „Swiss Finish“ dar. Die vorgeschlagene Regelung birgt erhebliche Risiken für Unternehmen, diese zu verletzen, da sie zu umfangreich ausgestaltet ist. Auf die verschärften Strafbestimmungen und Bussen wird nachfolgend näher eingegangen. Wir schlagen folgende Formulierung vor: „Profiling: jede **automatisierte** ~~Auswertung~~ **Bewertung** von Daten oder Personendaten, um wesentliche persönliche Merkmale **zu bewerten und** zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität. Die Auswertung von subjektiven Beurteilungen einer betroffenen Person stellt kein Profiling dar.“
RCH	DSG	3		h	Die Umschreibung des „Verantwortlichen“ ist für grössere Unternehmen zu generell und umfassend. Es ist darzulegen, ob hierunter die für die Unternehmung handelnde natürliche Person fällt und mit welchen Rechten und Pflichten der Verantwortliche bzw. die für die Unternehmung handelnde natürliche Person ausgestattet werden soll. Wir schlagen vor, dass die Umschreibung des „Verantwortlichen“ auf die Ebene der Unternehmung sowie auf die Ebene der für die Unternehmung handelnden Personen erweitert wird.
RCH	DSG	4	3		Die Definition eines „klar“ erkennbaren Zwecks führt in der Praxis zu Auslegungs- und Umsetzungsschwierigkeiten und führt nicht zu einem verbesserten Datenschutz für die betroffene Person. Wir schlagen folgende Formulierung vor: „Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.“
RCH	DSG	4	4		Die „Löschungsverpflichtung“ in Artikel 4 Abs. 4 ist zu konkretisieren (vgl. auch die Ausführungen zu Art. 3 lit. d). Ebenfalls soll eine Ergänzung bezüglich gesetzlicher Aufbewahrungspflichten eingefügt werden. Wir schlagen folgende Formulierung vor: „(… unverändert …) als der Zweck der Bearbeitung es bedingt, **ausser es bestehen gesetzliche Aufbe-**

					wahrungspflichten.“
RCH	DSG	4	5		In Absatz 5 wurde eine neue Pflicht zur Korrektur der Daten eingeführt. Die Umsetzung kann in der Praxis sehr aufwändig sein, insbesondere wenn die Daten von der Person aufgrund eines Vertrags selbst zur Verfügung gestellt worden sind. Wir schlagen folgende Formulierung vor: „Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. **Diese Pflicht entfällt, wenn die Daten von der betroffenen Person im Rahmen einer Geschäftsbeziehung bekannt gegeben wurden.** Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten unzugänglich zu machen, **ausser es bestehen gesetzliche oder aufsichtsrechtliche Aufbewahrungsvorschriften.**“
RCH	DSG	4	6		Die Ausgestaltung dieses Absatzes ist zu weitgehend. Zudem ist fraglich, ob das Schutzbedürfnis beim Profiling tatsächlich eine Ausdrücklichkeit erfordert. In jedem Fall muss eine solche Einwilligung in standardisierter Form vom Betroffenen eingeholt werden können. Wir schlagen folgende Formulierung vor: „(… unverändert …) wenn sie nach angemessener Information ~~freiwillig und eindeutig~~ erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss eine Einwilligung ~~zudem~~ erfolgen. **Diese Einwilligung ist in standardisierter Form möglich.**“
RCH	DSG	5	3	b/c	Aus dem Vernehmlassungsentwurf sowie dem Erläuterungsbericht geht nicht hervor, welche Unterschiede zwischen „spezifischen Garantien“ und „standardisierten Garantien“ bestehen. Es bedarf einer Präzisierung der Begriffe.
RCH	DSG	5	6		Die Informationspflicht gegenüber dem Beauftragten ist neu und der europäischen DSGVO nicht zu entnehmen. Der Transparenzgedanke steht in keinem Verhältnis zum sehr hohen administrativen Aufwand für Unternehmen. Wir schlagen die ersatzlose Streichung vor: ~~„Der Verantwortliche oder der Auftragsdatenbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmsinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit.~~

RCH	DSG	6	1	a	Der Begriff „Einzelfall“ hat in der heutigen Praxis zu Unklarheiten in der Anwendung geführt. Meistens wird die Einwilligung für einen Zweck eingeholt und nicht für eine einzelne Übermittlung. Deshalb soll dieser Begriff gestrichen werden: „a. die betroffene Person ~~im Einzelfall~~ eingewilligt hat;
RCH	DSG	6	2		Diese Informationspflicht geht ebenfalls weiter als die europäische DSGVO und führt für Unternehmen zu unverhältnismässigem Aufwand ohne den Datenschutz für die betroffene Person zu erhöhen. Wir schlagen die ersatzlose Streichung vor: ~~„Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.~~
RCH	DSG	7	2		Es ist im Gesetz selber nicht geregelt, welche weiteren Pflichten dem Auftragsbearbeiter überbunden werden sollen. Es wird auf eine Verordnung des Bundesrates verwiesen, deren Inhalt nicht bekannt ist. Wir schlagen vor, diesen Absatz wie nachstehend erwähnt zu ändern und die weiteren Pflichten direkt im DSG zu regeln: „(… unverändert…) zu gewährleisten. ~~Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters“.~~
RCH	DSG	7	3		In der heutigen arbeitsteiligen Welt ist das Verlangen nach einer „vorgängigen schriftlichen Zustimmung“ kaum umsetzbar. Wir schlagen folgende Formulierung vor: „Der Auftragsbearbeiter darf die Bearbeitung nur mit ~~vorgängiger schriftlicher~~ Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. Es soll genügend, dass der Übertragung von Anfang und generell abstrakt zugestimmt werden kann.
RCH	DSG	8			Es ist unklar, (i) welche Kompetenzen dem Beauftragten hiermit übertragen werden (ii) wie die Verfahren bezüglich Erstellung und Ausgestaltung solcher Empfehlungen aussehen (iii) welche rechtsstaatlichen Instrumente den Unternehmungen in diesem Kontext eingeräumt werden.

					Der Gesetzgeber muss die Kompetenzen des Beauftragten nachvollziehbar umschreiben (bspw. Vorgehen bei Dissens zwischen dem Beauftragten und den Unternehmen bei der Erstellung von Empfehlungen der „guten Praxis“) sowie die Art und Weise der Entstehung solcher Empfehlungen (bspw. welche generellen Verfahrensmöglichkeiten werden den Unternehmen zur Verfügung gestellt?) und deren Verbindlichkeit (bspw. welche Massnahmen sind bei einer allfälligen Verletzung der Empfehlungen der „guten Praxis“ seitens des Unternehmens einzuleiten?) regeln.
RCH	DSG	12			Der Umfang des Einsichtsrechtes ist nicht klar geregelt. Der Begriff „Daten“ bedarf einer näheren Ausführung resp. Beschreibung. Ein Einsichtsrecht zu gewähren kann mit hohem Aufwand verbunden sein. Ein solches Recht kostenlos anbieten zu müssen, stellt einen Eingriff in die unternehmerische Freiheit dar. Zudem führt ein kostenloses Einsichtsrecht dazu, dass Unternehmen zwangsläufig mit einer erheblichen Anzahl an Gesuchen konfrontiert werden. Dies kann nicht die Absicht des Gesetzgebers sein. Wir schlagen folgende Formulierung des Artikels 12 Absatz 1 vor: „Der Verantwortliche muss ~~kostenlos~~ Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und:“
RCH	DSG	12	1	a	Diese Bestimmung ist in der Praxis nicht umsetzbar, da die Feststellung der ausdrücklichen Untersagung der verstorbenen Person bezüglich Einsichtsrecht kaum erfolgen kann. Systemtechnisch müsste eine allfällige Untersagung abgebildet werden, um diese Bestimmung einhalten zu können. Wir schlagen die ersatzlose Streichung diese Bestimmung vor: ~~„a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder“~~
RCH	DSG	12	2		Diese Bestimmung ist nicht praxistauglich, da die Unternehmen die Feststellung einer „faktischen Lebensgemeinschaft“ nicht rechtsgenüglich feststellen kann. Im Bankenumfeld werden faktische Lebensgemeinschaften systemtechnisch nicht erfasst und können auch sonst nicht an Hand von Dokumenten plausibilisiert werden, gerade auch, um den Schutz der Persönlichkeit zu gewährleisten. Die Regelung birgt Potenzial für mögliche Datenschutzverletzungen, da der Verantwortliche das Bestehen einer faktischen Lebensgemeinschaft falsch beurteilt und Einsicht gewähren könnte. Wir schlagen die folgende Formulierung vor:

					„(… unverändert …) in eingetragener Partnerschaft lebten ~~oder mit ihr eine faktische Lebensgemeinschaft führten.~~“
RCH	DSG	12	3		Das Verhältnis von Art. 12 Absatz 3 zu Art. 47 Bankgengesetz ist dahingehend zu präzisieren, dass Art. 12 Absatz 3 als „lex specialis“ vorgeht.
RCH	DSG	12	4		Ein solch weitreichendes Recht soll lediglich durch die Erbengemeinschaft als Ganzes, ein von ihr bestimmter Erbenbevollmächtigter oder der alleinig Erbberechtigte ausgeübt werden können. Darüber hinaus bedarf es einer Klarstellung, dass ein Löschungsanspruch nicht besteht, wenn gesetzliche Aufbewahrungspflichten entgegenstehen. Wir schlagen folgende Formulierung vor: „ ~~Jeder Erbe~~ **Die Erbengemeinschaft, ein von ihr bestimmter Erbenbevollmächtigter oder der alleinig Erbberechtigte** kann verlangen, dass der Verantwortliche Daten des Erblassers kostenlos löscht oder vernichtet, ausser:“ a. Der Erblasser hat die zu Lebzeiten ausdrücklich untersagt; **oder** c. **es bestehen gesetzliche Aufbewahrungspflichten**
RCH	DSG	13	2/3		Absatz 3 statuiert eine Informationspflicht, die systematisch in Absatz 2 zu integrieren ist. Wir schlagen folgende Formulierung vor: „**Absatz 2 lit. d. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger der Personendaten.“**
RCH	DSG	13	4		Diese Bestimmung geht über die Regelung der europäischen DSGVO hinaus. Aus Sicht der betroffenen Person führt die Information betreffend die Identität und den Kontaktdaten des Auftragsbearbeiters nicht zu einem verbesserten Datenschutz. Es handelt sich zudem um einen unnötigen Mehraufwand für die Unternehmen, den es zu vermeiden gilt. Wir schlagen die ersatzlose Streichung dieses Absatzes vor: ~~„Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien der Daten, die er bearbeitet, mit.“~~

RCH	DSG	13	5		Diese Bestimmung geht ebenfalls über die Regelung der europäischen DSGVO hinaus und verunmöglicht in der Praxis jegliche Beschaffung von Daten bei Dritten. Unmittelbar nach der Beschaffung werden die Daten gespeichert und im Nachgang gelesen. Wir schlagen eine Anpassung von Artikel 13 Absatz in Anlehnung an die Regelung der europäischen DSGVO vor: „Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person **innerhalb von 3 Monaten** ~~spätestens bei der Speicherung der Daten~~ informiert werden; **oder werden die Daten beschafft, um mit der betroffenen Person zu kommunizieren, so muss die betroffene Person bei dem ersten Kontakt informiert werden; oder** werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.“
RCH	DSG	14			Artikel 14 verwendet die Begriffe „Daten“ und „Personendaten“ nicht konsistent.
RCH	DSG	14	2	a	Der Begriff „Speicherung“ soll mit „Beschaffung“ ersetzt werden. Ebenfalls sind beispielsweise Pflichten der Aufsichtsbehörde nicht in einem expliziten Gesetz festgehalten. „a. die ~~Speicherung~~ **Beschaffung** oder die Bekanntgabe der Daten ~~ausdrücklich~~ im Gesetz oder **in Regulierungen** vorgesehen ist, oder „c. **die Daten dem Amts- oder Berufsgeheimnis unterliegen.**“
RCH	DSG	14	4	a	Diese Bestimmung geht unnötigerweise über die Regelung der europäischen DSGVO hinaus und muss deshalb gestrichen werden. Wir schlagen folgende Formulierung vor: „a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt;~~
RCH	DSG	14	5		Diese Bestimmung ist wie folgt zu präzisieren. „(… unverändert …) das Aufschieben der Information **gemäss Absatz 3 oder 4** wegfällt, (… unverändert …).“
RCH	DSG	14	6		In der europäischen DSGVO ist eine Bestimmung eingefügt, welche offenkundig unbegründete oder exzes-

					sive Anträge regelt. Der Gesetzgeber muss eine vergleichbare Regelung aufnehmen. Nur so können „gleich lange Spiesse“ erzielt und Aufwandsgesichtspunkten Rechnung getragen werden. Wir schlagen folgende Regelung vor: **„Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder** **a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Massnahme berücksichtigt werden, oder** **b) sich weigern, aufgrund des Antrags tätig zu werden.** **Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.“**
RCH	DSG	16	1		Der Anwendungsbereich dieser Bestimmung ist zu offen formuliert, was Rechtsunsicherheit und hohe Umsetzungskosten verursacht. Wir schlagen folgende Formulierung vor: „Führt die vorgesehene Datenbearbeitung ~~voraussichtlich~~ zu einem **hohen** ~~erhöhten~~ Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder ~~der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.“
RCH	DSG	16	3		In der europäischen DSGVO ist lediglich der Verantwortliche von der Durchführung einer Datenschutz-Folgeabklärung betroffen. Eine vergleichbare Regelung ist unter Kostenaspekten und Gründen der Praktikabilität zwingend. Zudem muss der Beauftragte lediglich bei Fortbestehen eines hohen Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Person informiert werden. Wir schlagen folgende Formulierung vor: „Der Verantwortliche ~~oder der Auftragsdatenbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen, **wenn trotz der Massnahmen ein hohes Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person besteht.“**
RCH	DSG	16	4		Die Bestimmung regelt nicht, welche Massnahmen zu ergreifen sind, wenn der Beauftragte Einwände erhebt. Die Regelung ist wie folgt zu präzisieren:

					„(… unverändert …) so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit. **Der Beauftragte hat dem Verantwortlichen schriftlich mitzuteilen, welche Massnahmen zu ergreifen sind.“**
RCH	DSG	17	1		Der Anwendungsbereich dieser Bestimmung ist zu offen und zu weit formuliert, was Rechtsunsicherheit verursacht. Die Umsetzung dieser Regelung verursacht unnötige Kosten und verbessert den Datenschutz nicht. Wir schlagen die folgende Formulierung vor: „(… unverändert …) es sei denn die Verletzung des Datenschutzes führt ~~voraussichtlich~~ nicht zu einem **hohen** Risiko für die Persönlichkeit ~~und die Grundrechte~~ der betroffenen Person.“ Die gemeldete Verletzung wird nicht sanktioniert. Erfolgt die Meldung an den Beauftragten nicht fristgerecht, so ist ihr eine Begründung für die Verzögerung beizufügen.
RCH	DSG	17	4		Diese Bestimmung ist nicht kongruent zu Absatz 1 und entsprechend zu präzisieren: „Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung **oder einen Verlust von Daten.**“
RCH	DSG	19		a	Der Anwendungsbereich dieser Bestimmung ist unklar formuliert und schränkt die unternehmerische Freiheit der Unternehmungen zu stark ein. Wir schlagen folgende Formulierung vor: „a. Sie ~~dokumentieren ihre Datenbearbeitung~~ **führen ein Verzeichnis aller Verarbeitungsaktivitäten, die ihrer Zuständigkeit unterliegen.“**
RCH	DSG	20			Es ist abzulehnen, dass ein Auskunftsbegehren einer betroffenen Person kostenlos vom Verantwortlichen beantwortet werden muss. Für die Begründung, vgl. die Ausführungen zu Artikel 12.
RCH	DSG	20	2	b	Diese Bestimmung ist zu weitreichend formuliert und geht über die Bestimmungen der europäischen DSG-VO hinaus. Mit der jetzigen Formulierung müssen der betroffenen Person sämtliche Personendaten in einem Auskunftsbegehren bekannt gegeben werden. Die Beschränkung des Auskunftsrechts auf Kategorien von Personendaten ist ausreichend, da der betroffenen Person in einem 2. Auskunftsersuchen die einzelnen spezifizierten Personendaten ohnehin bekannt gegeben werden müssen. Wir schlagen folgende Formulie-

					rung vor: „b. die **Kategorien der** bearbeiteten Personendaten;“
RCH	DSG	20	2	f	Die Herkunft der Personendaten soll lediglich mitgeteilt werden, wenn diese nicht bei der betroffenen Personen erhoben wurden. Die vorgeschlagene Regelung führt nicht zu mehr Datenschutz und birgt keine neuen Erkenntnisse für die betroffene Person. Wir schlagen folgende Formulierung vor: **„f. wenn die verfügbaren Angaben über die Herkunft der Personendaten, sofern diese nicht bei der betroffenen Person erhoben wurden.“**
RCH	DSG	20	3		Dieser Absatz geht weit über die Bestimmungen in der europäischen DSGVO hinaus. Die Ausweitung auf jede Datenbearbeitung ist ein Eingriff in die operative Führung eines jeden Unternehmens und zwingt dieses, jede Entscheidung zu begründen. Wir schlagen die folgende Formulierung vor: ~~„Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine~~ **Bei** automatisierte**n** Einzelentscheidunge**n** erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung, soweit ihr dies nicht bereits mitgeteilt wurde.“
RCH	DSG	20	7		In der europäischen DSGVO ist eine Bestimmung eingefügt, welche offenkundig unbegründete oder exzessive Anträge regelt. In Anbetracht der Komplexität und des Aufwands bezüglich Beantwortung solcher Auskunftsbegehren muss der Gesetzgeber eine vergleichbare Regelung aufnehmen. Wir schlagen folgende Regelung vor: **„Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder** **a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Massnahme berücksichtigt werden, oder** **b) sich weigern, aufgrund des Antrags tätig zu werden.“** **Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.“**

RCH	DSG	23	2	d	Die Relevanz von Profiling muss auf automatisierte Einzelentscheidungen limitiert werden. Deshalb ist diese Bestimmung ersatzlos zu streichen. Sollte an dieser Regelung festgehalten werden, so ist die Ausdrücklichkeit zu streichen resp. muss klar sein, dass die Einwilligung in standardisierter Form (Allgemeine Geschäftsbedingungen) von der betroffenen Person eingeholt werden kann. ~~„d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person“~~
RCH	DSG	44	3		Das Fehlen der aufschiebenden Wirkung ist dahingehend neu zu formulieren, als dass die ordentlichen Verfahren und Prozesse zur Anwendung kommen sollen.
RCH	DSG	50ff.			Die Ausgestaltung des 8. Abschnittes (Strafbestimmungen) muss allgemeinen Strafrechtsgrundsätzen entsprechen. Die Bestimmungen sind in Art und Umfang, in der Formulierung, in der Konsistenz und in der Ausgestaltung des Strafmasses stark zu kritisieren. Bussen von bis zu CHF 250‘000 für fahrlässige Vergehen sind wirtschaftsschädlich für die Schweiz. Generell erheben wir folgende Kritik: (1) Natürliche Personen rücken im Rahmen der datenschutzrechtlichen Strafbestimmungen zu stark in den Fokus. Fahrlässigkeit eines Mitarbeitenden ist immer strafbar. Fahrlässigkeit unter Strafe ist unverhältnismässig und hat für die Umsetzung der Bestimmungen des DSG negative statt positive Folgen (überbordender Formalismus). (2) Es ist unklar, weshalb gewisse Tatbestände Antragsdelikte sind und andere nicht. Antragsdelikte sind meist leichtere Straftaten. Dies steht im Widerspruch zu den vorgesehenen Bussen bis zu CHF 250‘000. (3) Es ist unklar, wer bei Antragsdelikten Antragsteller ist (immer die betroffene Person?). (4) Es ist unklar, weshalb bei einigen Tatbeständen ausdrücklich natürliche Personen strafbar sind. Bedeutet dies, dass in diesen Fällen Artikel 53 nicht anwendbar ist? (5) Die Strafbarkeit des Unternehmens nach Artikel 53 ist anderes geregelt als in Art. 102 StGB. Dies führt zu Abgrenzungsschwierigkeiten und Rechtsunsicherheit. Economiesuisse hat einen Vorschlag für das Sanktionsmodell im DSG erarbeitet, in welchem nicht Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen im Vordergrund stehen. Die Stoss-

					richtung des Vorschlags erscheint uns im Grundsatz als nachvollziehbar. Der im Vorschlag erwähnte Ansatz des Anknüpfungspunkts „Organisationsmangel im Unternehmen“ ist unseres Erachtens jedoch nicht im Sinne der Unternehmen formuliert. Die Eintretenswahrscheinlichkeit eines Organisationsmangels ist im Vorschlag zu hoch und müsste eingeschränkt werden.
RCH	DSG	52			Die berufliche Schweigepflicht ist spezialgesetzlich geregelt und muss im Datenschutzgesetz nicht wiederholt werden. Wir schlagen die ersatzlose Streichung vor.
RCH	DSG	53			Die Ausgestaltung von Übertretungen und Vergehen in Geschäftsbetrieben ist mit Blick auf den Pönalisierungscharakter von Mitarbeitenden zu entschärfen. Wir schlagen die folgende Formulierung vor: „Übertretungen und **Vergehen** in Geschäftsbetrieben“ Von der Ermittlung der strafbaren Personen **wird** ~~kann~~ Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt ~~werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.“~~
RCH	DSG	54			Diese Bestimmung ist bereits in der Strafprozessordnung (StPO) geregelt. Es bedarf keiner eigenständigen Regelung im Datenschutzgesetz. Wir schlagen die ersatzlose Streichung vor.

Amstutz Jonas BJ

Von: Joachim Fauth <joachim.fauth@readersdigest.de>
Gesendet: Montag, 3. April 2017 15:29
An: Amstutz Jonas BJ
Betreff: Stellungnahme
Anlagen: AUSGEFÜLLT Formular-fuer-Stellungnahme_de_VE-DSG.doc

Sehr geehrter Herr Amstutz,

beigefügt erhalten Sie unsere elektronische Stellungnahme.

Mit freundlichen Grüßen

Geschäftsleitung/Recht

ppa. Joachim Fauth

==========
ppa. Joachim Fauth
Rechtsanwalt – Syndikus
Mitglied d. Geschäftsleitung
Verlag Das Beste GmbH, Geschäftsleitung/Recht
Vordernbergstr. 6, 70191 Stuttgart
Tel.: (0711) 6602-506 - Fax: (0711) 6602-136
e-mail: Joachim.Fauth@readersdigest.de
Amtsgericht Stuttgart HRB 723451
Geschäftsführer: Lutz Bode, Karsten Seidel
==========

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Das Beste aus Reader‘s Digest AG

Abkürzung der Firma / Organisation : RD

Adresse : Räffelstraße 11, CH-8054 Zürich

Kontaktperson : Joachim Fauth

Telefon : +49 711 6602 506

E-Mail : joachim.fauth@readersdigest.de

Datum : 03.04.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
RD	Insgesamt fällt bei Durchsicht des Gesetzesentwurfs auf, dass der grundsätzlich positive Ansatz des Schweizer Datenschutzgesetzes - anders als die EU- nicht mit dem Konstrukt des Verbots mit Erlaubnisvorbehalts zu arbeiten, in der Praxis kaum zu anderen, für die Wirtschaft positiveren Ergebnissen führt. An einigen Stellen gar nimmt das DSG für die Wirtschaft deutlich unfreundlichere Positionen ein, als es die DSGVO tut. Es erscheint beinahe so, wie wenn als gedankliche Vorlage der DSG-Revision die Parlamentsversion des DSGVO-Entwurfs gedient habe. Einige Regelungen waren in dieser extrem wirtschaftsunfreundlichen Parlamentsversion der DSGVO noch enthalten, wurden dann aber glücklicherweise im Rahmen der weiteren Beratungen im Europäischen Rat durch die Regierungen der Mitgliedstaaten herausverhandelt und finden sich so nicht mehr in der Endfassung des DSGVO. Leider scheint auch bei der DSG-Revision eine gewisse „Einwilligungsgläubigkeit“ vorzuliegen, die bekanntermaßen aber immer die großen Log-In-Giganten, google, facebook, Amazon, e-bay bevorzugt. Die Verschärfungen des DSG gegenüber der DSGVO lassen sich weder mit dem Argument, man wolle ein angemessenes Datenschutzniveau im Hinblick auf die Drittstaaten-Regelung der DSGVO schaffen, begründen, noch sind sie sonst rechtspolitisch nachvollziehbar.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
RD	DSG	1		e	**Art. 1 DSG e:** Als Ziel definiert Art. 1 lediglich den Schutz des Betroffenen. Demgegenüber formuliert die DSGVO einen Ziel-Dualismus. Die DSGVO nennt gleichgeordnet in Art. 1 Abs. 1 den freien Verkehr von Daten. Das DSG sollte diesen Interessenausgleich ebenfalls stärker betonen und nicht hinter der DSGVO zurückbleiben.
RD	DSG	3		a	**Art. 3 a VE-DSG:** Bei der Definition von Personen und Daten verweigert sich das Gesetz der Aufklärung, was unter Bestimmbarkeit der Person zu verstehen ist. In der Begründung wird in Anlehnung an die Erwägungsgründe der DSGVO bei der Frage, ob Drittwissen einbezogen wird, darauf abgehoben, ob vernünftigerweise solches Drittwissen wohl einbezogen werde. Eine weniger schlanke Definition im Gesetzestext erscheint sinnvoll, weil die Frage des Personalbezugs für das gesamte DSG von zentraler Bedeutung ist.
RD	DSG	3		f	Art. 3 f VE-DSG Die Definition von profiling erscheint uns in hohem Maße missglückt. Und sie geht weiter als das, was die DSGVO unter „profiling“ versteht. Während die DSGVO in Artikel 4 Nr. 4 schon in der Begriffsbestimmung immer einen Personenbezug fordert, verzichtet die Definition in Artikel 3 f VE-DSG hierauf. Auch nicht personenbezogene Daten werden vom profiling erfasst. Das ist insoweit signifikant, als Art. 4 Abs. 6 VE-DSG profiling generell nur bei Einwilligung zulässt. Die Selektion von Daten unter Zuhilfenahme von nicht personenbezogenen Daten wird also schon erfasst. Hierbei geht es wohlgemerkt nicht um ausführliche umfassende Persönlichkeitsbilder, die quasi den „gläsernen Betroffenen“ erzeugen, sondern um die einfache Verkettung personenbezogener und nicht personenbezogener Daten. Bei Lichte betrachtet, geschieht hier aber nichts anderes, als das, was in

					der analogen Welt schon zu Zeiten der Römer galt, nämlich dass Erfahrungswissen der Verkäufer einbezogen wird. Wenn in einer Datei vermerkt sird, dass Herr Müller bei gutem Wetter, insbesondere wenn die Temperatur über 25 ° steigt, eher geneigt ist, in der Eisdiele Eis zu kaufen, dann verkettet dies ein personenbezogenes Datum von Herrn Müller mit Wetterdaten. Schon diese triviale Verbindung eines personenbezogenen und eines nicht personenbezogenen Datums ist Profiling und würde nach der VE-DSG der Einwilligung bedürfen! Wenn mit der ausgedehnten Profiling-Regelung der “gläserne Betroffene“ verhindert werden sollte, dann wird hier mit den falschen Mitteln gekämpft. Die Verarbeitung von Daten muss nämlich nach Art. 4 Abs. 2 verhältnismäßig sein. Das ist sie nicht mehr, wenn sinnlos und weitschweifend Daten quasi "auf Vorrat" gesammelt werden, um solche umfassenden Profile zu erzeugen. Ein Autoverkäufer wird sich möglichst detailliert Daten zur Kaufkraft seiner Kunden und interessenspezifisch, welches Fahrzeug sie fahren, welche Kilometerleistung sie im Jahr haben etc. notieren. Die übrigen Lebensumstände, beispielsweise, ob sich der Kunde gesund ernährt, oder nicht, interessieren den Autoverkäufer nicht. Das Erfordernis der Verhältnismäßigkeit verhindert bereits Missbrauch.Im Gegenteil führt aber die enge Verkettung der Profiling-Definition mit Einwilligung dazu, dass die Log-In-Giganten massiv bevorzugt werden. Wenn jemand umfassende Persönlichkeitsprofile erstellen kann, dann sind es diese Log-In-Giganten, weil sie überhaupt erst in der notwendigen Breite das Verbraucherverhalten beobachten können. Ein google weiß nämlich nicht nur, ob sich ein Verbraucher nach einem neuen Auto erkundigt, sondern auch, wie dessen Ernährungsgewohnheiten sind. Das Autohaus wird über die Ernährungsgewohnheiten ohnehin nie etwas erfahren. Um aber beim Beispiel zu bleiben, ist es für google, Amazon und Co. aufgrund deren Struktur viel einfacher, über Log-in Mechanismen Einwilligungen beliebiger Art zu bekommen. Derjenige, der also hier die Möglichkeit hat, umfassende Profile zu erzeugen, wird durch die Logik, Einwilligung, ja die Gläubigkeit an das Allheilmittel der Einwilligung auch noch zusätzlich bevorzugt. Die DSGVO hat das jedenfalls in der letzten verabschiedeten Fassung besser geregelt. Profiling als solches ist zulässig und hängt von der Interessenwahrnehmungsklausel (Art. 6 Abs. 1f DSGVO) ab. Nur (!) in den Fällen, in denen das Profiling Teil einer automatischen Entscheidung wird, also rechtliche Wirkung erzeugt, beispielsweise die Kreditvergabe, gelten andere Vorschriften. Der VE-DSG vermischt leider automatische Entscheidung und profiling in höchst unglücklicher Weise und kommt zu einem Ergebnis, das weit strenger ist als die DSGVO.Die Schweizer Unternehmen werden massiv gegenüber dem europäischen Wettbewerber benachteiligt!

RD	DSG	4	3		**Art. 4 Abs. 3 VE-DSG:** Auffällig ist, dass die Zweckbindung in der VE-DSG auf einen Zweck begrenzt wird. Demgegenüber spricht die DSGVO in Art. 5 Abs. 1 b von mehreren Zwecken. Das ist mehr als eine sprachliche Unschärfe. Eindeutig ist damit die VE-DSG enger als die DSGVO.
RD	DSG	4	5		**Art. 4 Abs. 5 VE-DSG** Das Gebot der Datenüberprüfung sollte überprüft werden, jedenfalls dann, wenn dieses wie hier voraussetzungslos gefordert wird. Eine Eingrenzung der Korrekturverpflichtung auf die Fälle, in denen das Unternehmen positiv von der Fehlerhaftigkeit der Daten weiss, wäre angemessener.
RD	DSG	4	6		**Art. 4 Abs. 6 VE-DSG** Über diese Verkettung von automatischer Entscheidung und Profiling verweisen wir auf die Ausführungen zu Art. 3 f. Die DSGVO erlaubt - anders als der Entwurf - Profiling lediglich in Fällen einer automatischen Entscheidung, also wenn eine erheblich rechtliche Wirkung vorliegt. (Bsp. Kreditvergabe) steht dem Betroffenen das Recht zu, dass eine "reale Person" auf die Einschätzung einwirken kann (Art 22 III DSGVO). selbst in diesem Fall wird also gerade nicht eine Einwilligung verlangt! Die Vorschrift geht weit über die Regelungen der DSGVO hinaus.
RD	DSG	13	2		**Art. 13 Abs. 2 VE-DSG** Das Abheben auf den Zeitpunkt des Beschaffens in Art. 13 II muss geändert werden. Nach den Ausführungen in der Begründung (S. 57) sind damit auch Vorfeld-Maßnahmen umfasst. Sollte „beschaffen“ soweit verstanden werden, dass das Anmieten von Daten bei einem Drittunternehmen zur späteren Bewerbung schon als „Beschaffen“ gilt, dann wäre die Regelung in Art. 13 Abs. 2 fatal. Das würde nämlich bedeuten, dass bereits zum Zeitpunkt der Anmietung der spätere Werbeempfänger darüber informiert werden muss, dass er später beworben werden wird. Die DSGVO hat dafür eine, wie uns scheint, klarere Formulierung gefunden. In Artikel 14 Abs. 1 DSGVO wird nämlich auf den Akt des Erhebens Bezug genommen. Wenn also im Lettershop-Verfahren, bei dem der Adressvermieter die Adressen direkt dem Lettershop zur Verfügung stellt und das Erheben der Daten erst stattfindet, wenn der Kunde bestellt, auf das Erheben, sprich den Eingang der Bestellung abhebt, ist die Informationserteilung möglich und sinnvoll. Hier müssen die Informationen in der entsprechenden Werbung vorhanden sein. Und wenn der Beworbene dann eine Bestellung tätigt, oder sonst Kontakt mit dem werbenden Unternehmen aufnimmt, hat er die Informationen

					vorliegen. Die DSGVO hat für den Fall, dass Daten tatsächlich übermittelt (und nicht nur genutzt) werden, also das werbende Unternehmen vom Datengeber die Daten tatsächlich bekommt, um sie dann in einer Werbeaktion einzusetzen, eine durchaus sinnvolle Regelung zum Zeitpunkt der Information gefunden. In solchen Fällen der echten Übermittlung von Daten und damit im Grunde der Erhebung beim „Dritten, ordnet Art. 14 Abs. 3 a DSGVO an, dass die Information innerhalb einer "angemessenen Frist“ erfolgt. Das macht durchaus Sinn, denn wenn ein Unternehmen fremde Adressen von einem Dritten bekommt, um sie dann für eine Werbung einzusetzen, dann geschieht die Werbung ja zeitnah und damit kann die Information auch zeitnah erteilt werden. Selbstredend ist natürlich der „Informationskatalog“ in Art. 13 VE-DSG weit sinn- und massvoller als die Informationsschlacht, die in der DSGVO abgefeuert wird. Hier gilt es, dieses sinnvolle Maß in jedem Fall zu bewahren. Die Regelung sollte außerdem dahingehend ergänzt werden, dass die Information auch im Internet bereitgestellt werden kann. Wird z. B. ein Produkt im TV beworben und kann der Verbraucher über eine Bestellhotline direkt telefonisch bestellen, dann macht es keinen Sinn, Datenschutzinformationen im TV zu zeigen oder am Telefon vorzulesen. Auch bei kleinformatigen Anzeigen mit Bestellmöglichkeit ist es ausreichend, wenn eine Internetseite genannt wird, unter der die Datenschutzinformationen eingesehen werden können. Außerdem sollte generell für Informationsverpflichtungen eine Ergänzung aufgenommen werden, dass Informationen dann nicht erteilt werden müssen, wenn der Betroffene diese schon hat. Selbst die rigide DSGVO sieht das in Art. 14 Abs. 5 vor. Und es macht ja auch durchaus Sinn, Informationen nicht gebetsmühlenartig zu wiederholen, wenn sie der Betroffene ohnehin schon hat.
RD	DSG	15	1		**Art. 15 Abs. 1 VE-DSG** Die Schwelle, ab wann eine automatisierte Entscheidung vorliegt wird in Art. 15 Abs. 1 VE-DSG deutlich niedriger angesetzt, als dies in der DSGVO der Fall ist. in der DSGVO wird in Art. 22 Abs. 1 die automatisierte Einzelfallentscheidung wie dem Begriffspaar "rechtliche Wirkung" oder "in ähnlicher Weise erheblich beeinträchtigt" gekennzeichnet. nach der DSGVO handelt es sich also um eine erhebliche Beeinträchtigung. In dieser Formulierung wird deutlich, dass es sich um eine nachteilige Entscheidung handelt. Demgegenüber wählt Art. 15 Abs. 1 VE-DSG lediglich den Begriff der rechtlichen Wirkung bzw. der erheblichen Auswirkung. Die Beeinträchtigung, die Artikel 22 DSGVO fordert, findet sich in Art. 15 Abs. 1 VE-DSG nicht. Damit greift Art. 15 Abs. 1 VE-DSG schon dann ein, wenn die Entscheidung eine wertneutrale rechtliche Wirkung entfaltet.

					Demgegenüber stellt die DSGVO klar, dass es sich bei der Auswirkung um eine negative Beeinträchtigung handeln muss. Die von der DSGVO vorgenommene Entscheidung, nämlich dass nicht schon jede wertneutrale Entscheidung, sondern nur eine negativ beeinträchtigende Verpflichtungen des Verantwortlichen auslöst, erscheint nachvollziehbarer und im Ergebnis richtig. Jedenfalls sollte die Regelung in der Schweiz nicht strenger ausgebildet sein, als die in der DSGVO, weil damit Schweizer Unternehmen benachteiligt werden.
RD	DSG	19		b	**Art. 19 b VE-DSG** Nach dieser Vorschrift der VE-DSG muss jede Berichtigung, Löschung oder Vernichtung von Daten dem Betroffenen mitgeteilt werden. Das ist aus unserer Sicht eine fatale Vorschrift, die, wenn man die Begründung liest (Seite 65) wohl auf einem tragischen Irrtum beruht. Es macht natürlich überhaupt keinen Sinn, dass jede Änderung oder Löschung von Daten den Betroffenen mitgeteilt werden muss. Im täglichen Arbeitsprozess werden ständig Daten berichtigt, gelöscht oder vernichtet, z. B. weil ein Kunde bezahlt hat, erfolgt die Berichtigung dahingehend, dass die Forderung nicht mehr offen ist, oder wir löschen, oder vernichten Daten in regelmäßigen Abläufen, weil die Daten schlicht keine Relevanz mehr haben, z. B. bestimmte Auslieferungsdaten oder dgl. aus Produktversänden. Es wäre jetzt geradezu absurd, über diese Änderung jedes Mal dem Betroffenen eine Mitteilung zu senden. Diese absurde Regelung in der VE-DSG beruht offensichtlich auf der Fehlinterpretation von Art. 19 DSGVO. Der Anwendungsbereich des Art. 19 DSGVO ist extrem schmal und hängt zusammen mit dem vom Europäischen Gerichtshof in der google Spain-Entscheidung (C-131/12)postulierten Recht „vergessen zu werden“. In der DSGVO wird dieses Recht vergessen zu werden letztlich als Löschungsanspruch umgesetzt, wobei als Reminiszenz an den EuGH eine Besonderheit dann gilt, wenn der Verantwortliche für die Datenverarbeitung die Daten öffentlich gemacht hat, insbesondere im Internet. Hier gelten dann zusätzliche Verpflichtungen und eben in diesem Zusammenhang gilt dann nach Art. 19 die Verpflichtung, eine Löschung, Berichtigung und dgl. dem Betroffenen mitzuteilen. Art. 19 DSGVO stellt klar, dass diese Mitteilungspflicht ausdrücklich nicht gegenüber dem Betroffenen gilt, und nur dann einschlägig ist, wenn diese personenbezogenen Daten „offengelegt“ wurden. Mit anderen Worten: Wenn ein für die Datenverarbeitung Verantwortlicher personenbezogene Daten öffentlich gemacht hat, sprich im Internet veröffentlicht hat, (Art. 17 Abs. 2 DSGVO) dann teilt er den Empfängern dieser Information eine Berichtigung mit, sprich er berichtigt den entsprechenden Internet-Eintrag. Art. 19 VE-DSG macht daraus eine Berichtigungspflicht gegenüber den Betroffenen. Außerdem gilt Art. 19 VE-DSG

					voraussetzungslos. Bei jeder Änderung und dgl. von Daten sollte eine Benachrichtigung an den Betroffenen erfolgen. Die DSGVO knüpft aber die Informationsverpflichtung daran, dass der Betroffene von sich aus irgendwelche Löschungen, Berichtigungen und dgl. verlangt hat. Dies ergibt sich aus dem Verweis des Art. 19 DSGVO auf die Art. 16, 17 Abs. 1 und Art. 18 DSGVO. Der Betroffene muss also aktiv werden und erst dann kommt überhaupt in Betracht, dass der Verantwortliche nach Art. 19 VE-DSG überhaupt tätig werden muss. Und selbst dann richtet sich, wie gesagt, Art. 19 DSGVO auf ein Tätigwerden mit Blick auf die Öffentlichkeit und nur ausnahmsweise (Art. 19 DSGVO letzter Satz, bekommt der Betroffene eine Mitteilung, wenn er diese ausdrücklich verlangt hat. Die Regelung in Art. 19 VE-DSG erscheint das Resultat einer Missinterpretation der DSGVO und die Regel wäre eine schwere Bürde für die Schweizer Unternehmen.
RD	DSG	20	2	Satz 2	**Art. 20 Abs. 2 Satz 2 VE-DSG** Die Regelung verlangt, dass egal, was der Betroffene anfragt, er alle Informationen nach a-g der Aufzählung im Gesetzestext bekommt. Mit anderen Worten, der Gesetzestext verpflichtet zur Überinformation. Dabei geht der Text insoweit sogar über die weitschweifigen Regelungen der DSGVO (Art. 15) hinaus. Nach Art. 15 Abs. 1 Satz 1, zweiter Satzteil (DSGVO), hat der Betroffene, nämlich nur ein Recht darauf, Auskunft „über… folgende Informationen“ zu bekommen. Das heißt, wenn der Betroffene sich nach der Herkunft der Daten erkundigt, dann hat er ein Recht darauf, dieses zu verlangen. Anders, im Falle der Regelung im VE-DSG. Wenn er hier was auch immer fragt, bekommt er das volle Set der Antwort nach a-g. Diese Regelung ist überschießend und in dieser Form unnötig. Schweizer Unternehmen werden gegenüber der DSGVO benachteiligt.
RD	DSG	20	3		**Artikel 20 Abs. 3 VE-DSG** Artikel 20 Abs. 3 VE-DSG ist insoweit unglücklich formuliert, als es zunächst einmal jedes Ergebnis einer Datenverarbeitung erfasst. Dies ergibt sich durch die unglückliche Anfügung des „insbesondere Zusatzes“, der sich dann auf die automatisierte Einzelentscheidung bezieht. Der Grundsatz von Art. 20 Abs. 3 ist aber, dass über das Ergebnis jeder Entscheidung einer Datenverarbeitung zu informieren ist. Nimmt man das ernst, droht der Schweizer Wirtschaft ein Informations-Gau. In einem Unternehmen das eine Werbeselektion vornimmt, wird ein erheblicher Teil der Daten wohl nicht für eine Werbung in Betracht kommen, weil aufgrund der Datenlage man davon ausgeht, dass der Betroffene am Werbeangebot kein Interesse hat. Praktisches Beispiel: Wenn ein Unternehmen, das sowohl im Versandhandel, als auch im stationären Handel tätig ist, in Zürich eine neue Filiale eröffnet, dann wird es möglicherweise seinen Versandhandelskunden in Zürich eine Werbung

					zukommen lassen, die auf diese Neueröffnung hinweist. Diese Werbung auf die Neueröffnung in Zürich wird natürlich allen anderen Kunden des Unternehmens in St. Gallen, Chur etc. nicht zugehen, weil ernstlich wohl niemand von dort anreist, um sich die Filiale anzusehen. Datenschutzrechtlich gesehen, handelt es sich hier ja natürlich um eine datenschutzrechtliche Entscheidung, nämlich dass die Kunden in St. Gallen keine entsprechende Werbung erhalten. Nimmt man jetzt die Formulierung in Art. 20 Abs. 3 ernst, dann müsste das Unternehmen seinen Kunden in der restlichen Schweiz mitteilen, dass sie leider für das Werbeschreiben hinsichtlich der Neueröffnung in Zürich nicht in Betracht kamen, weil man davon ausgehe, dass es sie nicht in ausreichendem Maße interessiere. Das Ergebnis erscheint absurd. Auch hier wären Schweizer Unternehmen gegenüber der DSGVO deutlich benachteiligt!
RD	DSG	24	Nr. 2c	Nr. 3	**Art.24 Nr. 2 c Nr. 3 VE-DSG** Die Vorschrift lässt ein Kreditscoring nur bei volljährigen Personen zu. Hierbei geht der Minderjährigenschutz weiter als in der DSGVO. Artikel 8 DSGVO schützt Kinder maximal bis zu einem Alter von 16 Jahren. Die Nationalstaaten haben sogar das Recht, diesen Schutz bis auf das Alter von dreizehn Jahren herabzusetzen. Wie auch immer man das wendet, das apodiktische Verbot des Kreditscorings für Nichtvolljährige ist in der DSGVO so nicht abgebildet. Letztlich ließe sich über die Interessenswahrungsklausel ja auch vertreten, dass Geschäfte mit Kindern eben an anderen Maßstäben zu messen sind. Auch da wird man aber den besonderen Schutz jedenfalls nach DVO mit sechzehn enden lassen.
RD	DSG	22			**Schutz der Presse Artikel 22 VE-DSG** Der Gesetzgeber wählt hier einen eher selektiven Schutz als Ansatz. Artikel 22 Abs. 1 c. weist der Presse nur dann einen Schutz zu, wenn durch die Anwendung des Datenschutzrechtes die Meinungsfreiheit des Publikums gefährdet würde. Das bedeutet nichts anderes, als dass der Presse im Grunde genommen die Beweislast dafür auferlegt wird, dass bei Verarbeitung bestimmter Daten man redaktionell etwas „auf die Beine stellen“ wird, was der freien Meinungsbildung des Publikums dient. Die datenschutzrechtliche Privilegierung der Presse darf nicht erst dann einsetzen, wenn die Datensammlung in einen redaktionellen Beitrag mündet. Es ist das Wesen der Presse, dass sie das politische und gesellschaftliche Geschehen und die Akteure beobachtet. Dazu gehört wesensimmanent das Sammeln von Informationen. Ob zu einem späteren Zeitpunkt dann daraus ein

					redaktioneller Beitrag entsteht, oder nicht, ist in der Regel zum Zeitpunkt des Sammelns der Information überhaupt nicht zu klären. Würde man, wie dies Art. 22 VEDSG tut das Sammeln der Information davon abhängig machen, dass diese notwendig ist, um einen redaktionellen Beitrag zu erstellen, so würde die Presse auf eine "Rumpfberichterstattung" reduziert. Der Schutz der Presse muss bereits eingreifen, wenn diese Informationen in Ausübung ihrer redaktionellen Tätigkeit sammelt. Hierbei ist die redaktionelle Tätigkeit aber eben nicht erst die Veröffentlichung eines redaktionellen Beitrags, sondern das Beobachten des Geschehens und das Sammeln von Informationen ist selbst bereits Kernaufgabe der Presse. Zu Recht hebt z. B. das deutsche Bundesdatenschutzgesetz in § 41 insgesamt auf die journalistisch/redaktionelle Tätigkeit ab ohne die Eingrenzung, dass die freie Meinungsbildung sonst gefährdet würde. Auch die DSGVO nimmt diese Eingrenzung in Art. 85 nicht vor. Insbesondere fehlt der Gefährdungstatbestand, wie er in Art. 22 Abs. 1 Lit. c enthalten ist, völlig. Artikel 85 Abs. 1 DSGVO hebt allgemein auf die Tätigkeit der Presse zu journalistischen Zwecken ab. Die Schweizer Presse sollte gegenüber der europäischen Presse nicht benachteiligt werden.
RD	DSG	23			**Art. 23** unterwirft den unmittelbar Handelnden, also den Mitarbeiter im Unternehmen einem Straftatbestand. Damit gibt der Entwurf einen völlig anderen Weg, als dies die DSGVO gewählt hat. Die DSGVO hebt in ihren Sanktionsvorschriften auf denjenigen ab, der wirtschaftlich verantwortlich ist, nämlich das Unternehmen. Die Sanktionsvorschriften richten sich durchweg gegen das Unternehmen selbst. Die durch Art. 23 VE-DSG begründete persönliche Haftung des Mitarbeiters bringt diesen zudem in einen unerträglichen Interessenkonflikt, denn der Mitarbeiter ist arbeitsrechtlich zu einer Treue gegenüber dem Arbeitgeber verpflichtet, sieht sich jetzt aber durch eine persönliche Haftung in einen schwerwiegenden Loyalitätskonflikt gestürzt.Im Übrigen überzeugt die persönliche Haftung des Mitarbeiters auch deshalb nicht, weil damit im Ergebnis der einzelne handelnde Mitarbeiter eine persönliche Verpflichtung auferlegt wird, wie sie normalerweise nur Berufsgeheimnisträgern persönlich auferlegt ist. Dass ein Rechtsanwalt oder Arzt eine persönliche Geheimhaltungspflicht aus seinem Berufsstand zu wahren hat, ist Teil der beruflichen Ausrichtung. Bei einem Mitarbeiter, der als Sachbearbeiter Datenverarbeitung vornimmt, ist dies gerade nicht der Fall. Es ist rechtspolitisch nicht nachvollziehbar, warum im Ergebnis ein solcher Sachbearbeiter wie Berufsgeheimnisträger persönlich in die Haftung genommen wird. Die persönliche Haftung des

					Mitarbeiters erscheint auch zum Schutz der Betroffenen nicht notwendig, denn ein Sanktionierungssystem kann, wie dies in der DSGVO auch seinen Niederschlag gefunden hat, sich gegen das Unternehmen selbst richten. Der VE-DSG sollte keine persönliche Haftung über die Sanktionierungssysteme in der DSGVO vornehmen.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Michael Eugster <michael.eugster@rembrand.ch>
Gesendet: Montag, 3. April 2017 16:38
An: Amstutz Jonas BJ
Betreff: Stellungnahme VE-DSG
Anlagen: Formular-fuer-Stellungnahme_de_VE-DSG.doc

Kategorien: Rote Kategorie

Sehr geehrter Herr Amstutz

In der Anlage übersenden wir Ihnen unsere Stellungnahme zum Vorentwurf des DSG.

Für Rückfragen stehe ich gerne zur Verfügung.

Freundliche Grüsse

Michael Eugster
Beratung | Projektleitung

Rembrand AG
Sonnengartenstrasse 6 | CH-9000 St.Gallen
Telefon +41 (0) 71 228 41 99 | Telefax +41 (0) 71 228 40 60
michael.eugster@rembrand.ch | http://www.rembrand.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Rembrand AG

Abkürzung der Firma / Organisation : REM

Adresse : Sonnengartenstrass 6, 9000 St.Gallen

Kontaktperson : Michael Eugster

Telefon : 071 228 40 50

E-Mail : michael.eugster@rembrand.ch

Datum : 3.4.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
REM	Grundsätzlich: Wir sind ein KMU, wir verstehen nicht warum der vorliegende Entwurf zur Totalrevision des DSG ggü. der EU-DSGVO und dem E-SEV 108 verschärft wurde und wir können uns diese Änderungen resp. neuen Bestimmungen gar nicht leisten. Die Modernisierung des DSG an die neuen technischen Möglichkeiten und die Annäherung an die künftige Rechtslage der EU ist begrüssenswert. Allerdings sind die Bemühungen, der Totalrevision den "Schweizer-Stempel" aufzudrücken, in unserem Fall in höchstem Masse geschäftsschädigend. Denn mit dem vorliegenden Entwurf erfolgt eine Legiferierung auf Vorrat. Eine solche ist weder notwendig noch wünschenswert. Die vorgeschlagene Änderung hinsichtlich der überaus zentralen Einwilligung zur Speicherung/Verarbeitung von persönlichen Daten – auch unter Einbezug des erläuternden Berichts – ist unklar. Ebenfalls ist die vorgesehene Dokumentationspflicht und das Auskunftsrecht für unser Unternehmen administrativ und finanziell gar nicht erst zu bewältigen. Die generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling stellt für uns eine der problematischtes Verschärfungen dar und ist in unseren Augen ein Jobkiller für die Schweizer Werbebranche. Auch das vorliegende Saktionssystem erachten wir in dieser Form als inakzeptabel. Es hat eine weitgehende Kriminalisierung von datenverarbeitenden Mitarbeitern in kleineren Organisationen zur Folge, als die gewünschte Disziplinierung der wirtschaftlich grossen teils auch internationalen Unternehmen. Es führt in unseren Augen auch zu einer massiven Benachteiligung von Schweizer Unternehmen ggü. internationalen Grossunternehmen, da die Vollstreckung im Ausland sowieso nicht möglich sein wird. Wir erachten den vorliegenden Entwurf des DSG als absolut KMU-feindlich und lehnen ihn in dieser Fassung ab.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
REM		3			Unter Einbezug des erläuternden Berichts ist die vorgeschlagene Regelung für uns unklar. „Personendaten“ soll gemäss Bericht inhaltlich nicht geändert werden. Im Bericht wird aber eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder eine Online-Identität“ identifiziert werden kann. Dies ist doch für sämtliche Online-Aktivitäten widersprüchlich. Denn heute gilt, wenn Angaben bloss einer bestimmten „eindeutigen Kennung“ oder „Identifikationsnummer“, wie z.B. einer IP-Adresse oder Cookie-Kennungen zugeordnet werden können, hinter welcher letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann. Somit wäre der Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites gar nicht mehr möglich. IP-Adressen werden heute mit Hilfe von Cookies bereits weiterverarbeitet, aber nicht im Interesse an der namentlichen Identifizierung der Person, sondern lediglich der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten, sodass letzten Endes zahlreiche heute werbefinanzierte, unentgeltliche Angebote künftig nicht mehr allgemein zur Verfügung stehen würden.
REM		4	5		Jeden Datensatz auf Richtigkeit zu überprüfen, würde zu erheblichen administrativen Mehraufwänden führen, die nicht zu tragen wären. Wir lehnen dies ab.
REM		4	6		Der zentrale Begriff "Einwilligung" ist unklar. Was heisst "Einwilligung"? Wie genau wir "eingewilligt"? Gerade hinsichtlich der Verwendung von Personendaten für Werbemassnahmen und Profiling ist dieser Begriff genau zu definieren und die Massnahmen dafür abschliessend aufzuzählen. Bitte auch festlegen, dass eine Einwilligung auch durch Zustimmung zu einem separaten Dokument (z.B. AGBs, Datenschutzbestimmungen), das die nötigen Informationen enthält, erteilt werden kann. Sie können ja nicht verlangen, dass bspw. auf Websites unter jedem Action-Button eine 10 seitige Erklärung

					abzugeben ist.
REM		8			Das Genehmigungsverfahren kann nicht dem EDÖB alleine unterliegen. Die Genehmigungsinstanz ist genau zu definieren und zu erweitern. Die Kompetenz des EDÖB zum eigenständigen Erlass von Empfehlungen ist problematisch. Jedenfalls muss den betroffenen Unternehmen hier eine Anfechtung ermöglicht werden. Bitte klare Regelung der Rechtsmittel ergänzen. Bitte auch klarstellen, wer zu den interessierten Kreisen gehört. Ein Mitwirken von Konsumentenverbänden muss ausgeschlossen werden, da deren Interessen bereits durch den EDÖB ausreichend berücksichtigt werden. Ein Rechtsmittel gegen die Genehmigungsentscheide ist ebenfalls vorzusehen.
REM		13	2		Bei einem Zugriff auf eine Website wird in den meisten Fällen IP und auch andere Informationen des Nutzer in Logfiles gespeichert. Technisch ist es nicht möglich, den Nutzer vor dem Zugriff auf eine Website darüber zu informieren. Deshalb bitte klarstellen, dass die ausreichend kenntlich gemachte Information in einer Datenschutzerklärung nach Abruf der Website als rechtzeitig gilt.
REM		13	3		Bitte abschliessende, schlanke Aufzählung der mitzuteilenden Informationen ausarbeiten.
REM		13	4		Ist ersatzlos zu streichen, da in der EU-DSGVO nicht vorgesehen und keinen Mehrwert für den Betroffenen. Bedeutet lediglich hohen administrativen Aufwand.
REM		13			Die Informationspflichten gehen generell viel zu weit, ohne dem Betroffenen einen Mehrwert zu bieten. Folglich sollte die Regelung darauf beschränkt werden, dass nur auf Nachfrage die Informationen geliefert werden müssen.
REM		15			Die Regelung geht wiederum viel zu weit. Die vorgesehenen Massnahmen in der EU-DSGVO (Art. 22) sind genügend und sollen übernommen werden.
REM		16			Der Anwendungsbereich ist unklar. Wann besteht ein erhöhtes Risiko? Aus diesem Grund ist die Massnahme auf grosse Risiken zu beschränken. In der Praxis bedeutet das auch ein erheblicher administrativer Mehraufwand, der nur bei grossen Risiken gerechtfertigt ist.

REM		17			Geht wiederum weiter, als für den Schutz des Betroffenen notwendig ist. Bei den vorgesehenen Sanktionsregelung, welche auf die Betrafung natürlicher Personen beruht, wird sich kaum jemand getrauen, der Kenntnis von einer Verletzung erlangt, dies zu melden. Der psychische Druck wird auf die betroffene Person immens sein. Denn entweder denunzieren Sie einen Arbeitskollegen oder machen sich gar selbst strafbar. Bei den ruinösen Strafbeträgen wird dies nicht funktionieren. Es ist auch unklar, durch wen die unbefugte Datenbearbeitung erfolgt. Sind damit Dritte (Hacker, Vertragspartner, die trotz Verbot die Daten bearbeiten etc.) gemeint? Bitte abschliessend aufführen. Wenn der Verantwortliche weiss, dass eine beabsichtigte Datenbearbeitung den Datenschutz verletzt, darf er sie gar nicht erst durchführen. Eine Meldung an den Beauftragten ist daher wenig sinnvoll. Ebenfalls schwierig zu beurteilen ist, wann ein Risiko für die Persönlichkeit vorliegt. Dies kann nicht immer abgeschätzt werden. Der einhergehende Mehraufwand (Einführung neuer Prozesse etc.) ist angesichts einer kaum möglichen wirksamen Umsetzung unverhältnismässig.
REM		18			Privacy by Default und Privacy by Design ist deshalb schon problematisch, weil deren Verletzung wiederum unmittelbar sanktioniert werden soll. Es gibt nicht eine einzige richtige Vorgehensweise. Es sind „angemessene Massnahmen“ bzw. „geeignete Voreinstellungen“ vorzunehmen. Hier muss ein gewisser Ermessensspielraum eingeräumt werden. Dieser ist klarzustellen. Ansonsten wäre die Sanktionierung insbesondere mit Blick auf das angedachte Sanktionssystem absolut unfair.
REM		19			Diese Dokumentationspflicht geht viel zu weit und können wir uns als KMU gar nicht leisten. Die Regelung darf keinesfalls über die in der EU-DSGVO Art. 30 abgefassten Punkte hinausgehen.
REM		19	b		Ist ersatzlos zu streichen.
REM		20			Das hier abgefasste Auskunftsrecht ist geradezu uferlos und ruinös. Es muss möglich sein, eine angemessene Aufwandsentschädigung zu verlangen. Zudem stellt sich die Frage, inwiefern ein Auskunftsrecht geltend gemacht werden kann, wenn die Daten bpws. über ein Kunden-Login

					eingesehen und bearbeitet werden können. Auch hier sind die Vorgaben der EU-DSGVO (Art. 19, 15) nicht zu überschreiten.
REM		23			Die ausdrückliche Einwilligung für das Profiling ist eine der problematischsten Schweizer Verschärfungen und ist zwingend zu streichen. Für uns als Werbedienstleister hat diese Anforderung erhebliche Konsequenzen und wird Arbeitsplätze kosten, weil diese Vorschrift jede Form von personalisierter Werbung und Marketing Automation verbietet. Denn nach dem E-SEV 108 ist eine entsprechende Vorgabe nicht verlangt. Auch nach der EU-DSGVO nicht für jegliche Form des Profiling. Es besteht keine Notwendigkeit, das Profiling per se als Persönlichkeitsverletzung einzustufen. Solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll.
REM		24	2		Zu ergänzen: Direktwerbung kann ein überwiegendes Interesse darstellen. Zudem verstehen wir den Begriff "möglicherweise" nicht. Eine Aufzählung soll abschliessend sein und eine gewisse Rechtssicherheit geben. Hier heben Sie mit diesem Wort diese Sicherheit wieder auf.
REM		50 ff.			Mit diesen Bestimmungen schiesst man völlig über das Ziel hinaus und wir lehnen sie gänzlich ab. Ein fahrlässiger Verstoss gegen das DSG soll künftig gleich massiv geahndet werde, wie die fahrlässige Verletzung des Bankgeheimnisses? Hingegen ist die fahrlässige Verletzung des Amts-, Anwalts- und Arztgeheimnisses nicht strafbar? Dies belegt doch eindrücklich die Unsinnigkeit dieser neuen Vorschriften. Zudem ist der persönliche, strafrechtliche Charakter der Sanktionen nicht zielführend. Die exponierten Personen, insbesondere die Datenschutzverantwortlichen, werden durch die neue Gesetzgebung nicht gestärkt, sondern massiv geschwächt und durch die Schaffung eines persönlichen Strafbarkeitsrisikos, welches das Leben dieser Personen und insbesondere das ihrer Familien finanziell faktisch ruiniert, unter massiven psychischen Druck gesetzt. Es werden sich keine guten Mitarbeiter mehr finden, die diese Verantwortung tragen wollen. Und kein innovatives Unternehmen wird bereit sein, seine Mitarbeiter diesen drastischen strafrechtlichen Risiken auszusetzen. Dieses Sanktionssystem ist in höchstem Mass innovationshemmend, reduziert die Agilität

					von Schweizer Unternehmen auf ein Minimum und sind für ein KMU gar nicht erst tragbar, was unweigerlich zu einem erheblichen Standortnachteil Schweiz führt. Somit ist auch der gesamte Schweizer Wohlstand gefährdet. Denn die KMU's bilden bekanntermassen das Rückgrat der Schweizer Wirtschaft. Mitarbeiter in den Unternehmen werden sich hüten, bei strafrechtlich bedrohten Datenschutzfragen selbst Entscheide zu fällen und werden sich über Rechtsdienste entsprechend absichern müssen. Die verteueren die sowieso schon hohen Dienstleistungspreise in der Schweiz zusätzlich und unnötig, worauf wiederum weitere Arbeiten durch günstigere ausländische Dienstleister erledigt würden. Denn diese Sanktionen werden ggü. Unternehmen ausserhalb der Schweiz sowieso nicht durchzusetzen sein. Das Ziel sollte doch sein, durch die Datenschutzbeauftragten in den Unternehmen für einen höheren Datenschutz zu sorgen. Aber diesen Job wird aus reinem Selbstschutz niemand mehr machen wollen. Und wenn denn, ist eine gewissenhafte Tätigkeit aufgrund dieser massiven Bussenandrohung gar nicht möglich. Sollte mal was passieren, wird wohl alles daran gesetzt, das Ganze unter den Teppich zu kehren oder dem nächstbesten „Bauernopfer“ anzuhängen.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
REM	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
REM	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
REM		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
REM		

Ringier | We inform. We entertain. We connect.

per E-Mail an: jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Zürich, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Im Dezember 2016 haben Sie uns eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Die Ringier AG reicht hiermit in der Beilage ihre Stellungnahme innerhalb der vom Bundesamt für Justiz angesetzten Frist ein und gibt der Hoffnung Ausdruck, dass im weiteren Gesetzgebungsverfahren den darin festgehaltenen Überlegungen Rechnung getragen werden kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Ringier AG

Adrian Dudle
Chief Legal Officer

Chantal Imfeld-Matyassy
Data Protection Officer

Ringier AG
Dufourstrasse 23
CH-8008 Zürich
Schweiz

T +41 44 259 61 11
F +41 44 259 68 40
www.ringier.com

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Ringier AG

Abkürzung der Firma / Organisation : RIN

Adresse : Dufourstrasse 23, 8008 Zürich

Kontaktperson : Chantal Imfeld-Matyassy, Data Protection Officer

Telefon : 044/259 85 79

E-Mail : chantal.imfeld@ringier.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
RIN	**1. Konzeption der Schweizer Datenschutzgesetzgebung vs. die Gesetzgebung der EU** Die Schweizer Datenschutzgesetzgebung basierte bis anhin grundsätzlich auf einem liberalen Ansatz und hat – so auch in der Schweizer Bundesverfassung verankert – den Persönlichkeitsschutz, die persönliche Freiheit und das informationelle **Selbstbestimmung**srecht des Bürgers im Fokus. Datenbearbeitungen sind grundsätzlich und unter Einhaltung bestimmter Voraussetzungen erlaubt: Einhaltung der Grundprinzipien gemäss Art. 4 DSG (Rechtmässigkeit, Treu und Glauben, Zweckbindung, Transparenzprinzip, Verhältnismässigkeitsprinzip, Legitimation der Bearbeitung durch einen Rechtfertigungsgrund, insbesondere die Einwilligung). Die Datenschutz-Gesetzgebung der EU hat einen genau gegenteiligen Ansatz. Die Datenbearbeitung ist grundsätzlich verboten. Es handelt sich also um ein Verbotsgesetz und nur unter dem Vorbehalt einer Erlaubnis dürfen Daten bearbeitet werden (Einwilligung, gesetzliche Pflicht oder überwiegendes Interesse, als Resultat einer Interessenabwägung). Durch die starke, teilweise sogar überschiessende Anpassung des VE-DSG an die DSGVO ist nun ein Entwurf entstanden, der aus einem Gesetz mit einem liberalen Ansatz mit Fokus Persönlichkeitsschutz und **Selbstbestimmung**srecht des Bürgers ein Verbotsgesetz macht. Die Veränderung der grundlegenden Konzeption unseres Datenschutzgesetzes würde deshalb wahrscheinlich zu einem Widerspruch zu unserer grundlegenden Konzeption der Gesetzgebung führen. Dieser Ansatz der Veränderung der Konzeption des Datenschutzgesetzes ist deshalb nicht zu begrüssen. Hinzu kommt, dass der Bürger im Hinblick auf sein in der Bundesverfassung verankertes Selbstbestimmungsrecht doch weitgehend entmündigt wird. Betrachtet man die Entwicklungen im Gesundheitsbereich (E-Health, Patientendossier), in welchem Bereich die Selbstbestimmung dem Bürger durchaus zugetraut wird, stellt sich unbestritten die Frage, wieso man dies dem Bürger im Sektor der kommerziellen Bearbeitung von Personendaten nicht auch weiterhin zutraut. Im Patientendossier wird dem Patienten auch vollumfänglich überlassen, dass er seine (besonders schützenswerten) Daten selbst verwaltet und selbst bestimmt, wer auf diese Daten Zugriff hat und was damit gemacht wird. Es stellt sich schon die Frage, wieso gerade im Bereich der Bearbeitung von Persönlichkeitsprofilen, die bis anhin genauso behandelt wurden wie die besonders schützenswerten Daten und auch denselben strengen Voraussetzungen unterlagen (Artt. 4 Abs. 5, 7 DSG, letzterer i.V.m. Artt. 8-11 u. 20-21 VDSG), der Bürger plötzlich scheinbar entmündigt wird und vermeintlich durch ein derart strenges Gesetz geschützt werden muss. Es ist nicht nachvollziehbar, dass personalisierte Werbung, welche nicht einmal eine Singularisierung bedingt, als ein schlimmerer Eingriff in die Persönlichkeit eines Bürgers gewichtet wird, als die Einsicht in seine Gesundheitsdaten. Das Potential einer Persönlichkeitsverletzung aufgrund des Letzteren ist aufgrund von Unwissen und Fahrlässigkeit durchaus höher einzustufen, da die Einstellungen der Zugriffmöglichkeiten beim Patientendossier dem Patienten überlassen werden. Es würde deshalb begrüsst werden, wenn auch im Sektor der kommerziellen Bearbeitung von Personendaten dem Bürger erlaubt werden würde, sein Selbstbestimmungsrecht selbstständig ausüben zu können.

RIN	**2. Benachteiligung von Schweizer Unternehmen gegenüber ausländischen Unternehmen** Gewisse Regelungen im VE-DSG (s. unten im Detail) sind umfassender als in der europäischen DSGVO und/oder in der Europarats-Konvention (E-SEV 108) oder mit Blick auf die Angemessenheits-Beurteilung des Schweizer Datenschutzrechts durch die EU nicht zwingend geboten (sogenanntes „Swiss-Finish"). Ein Datenschutzgesetz mit einem derartigen Swiss Finish würde bedeuten, dass die Zusammenarbeit sowie der grenzüberschreitende Datenfluss zwischen der Schweiz und den Unternehmen in der EU unnötig erschwert werden würde. Was eine Benachteiligung der Schweizer Unternehmen gegenüber den Unternehmen in der EU und letztlich eine Einschränkung der Wettbewerbsfähigkeit und des Wirtschaftsstandortes Schweiz bedeuten würde. Da die Schweizer Unternehmen bereits heute gegenüber Unternehmen, die in Ländern mit einem tieferen Datenschutzniveau agieren, benachteiligt sind, würde es begrüsst werden, wenn die Schweiz und ihre Unternehmen nicht noch stärker benachteiligt werden würden.
RIN	**3. VE-DSG vs. Digitale Strategie des Bundes**? Gemäss dem erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (im Folgenden „erläuternder Bericht", S. 8 f.) wird festgehalten, dass mittels der bundesrätlichen Strategie „Digitale Schweiz" die zunehmende Digitalisierung noch konsequenter genutzt werden und sich die innovative Volkswirtschaft noch dynamischer entwickeln soll. Integraler Bestandteil der bundesrätlichen Strategie „Digitale Schweiz" ist die Entwicklung einer Datenpolitik. Im Rahmen dieser Datenpolitik soll die Schweiz über kohärente Rechtsgrundlagen zu Daten und den Umgang mit ihnen verfügen und sich als attraktiven Standort für eine Wertschöpfung durch Daten positionieren. Zu diesem Zweck hat der Bundesrat an seiner Sitzung vom 22. März 2017 übergeordnete Ziele definiert und die Bundesverwaltung beauftragt, erste Eckwerte einer Datenpolitik zu entwerfen. Er stellte dabei auch fest, dass Daten der Rohstoff einer digitalen Wirtschaft und Gesellschaft sind. Geeignete Datenbestände sollen deshalb für eine Wiederverwendung zur Verfügung stehen. Der vorliegende Entwurf zum DSG mit den geplanten Verschärfungen von Informations- und Dokumentationspflichten, den Vorgaben Privacy by Design und Privacy by Default, der sehr restriktiven Definition von Profiling und der Vorgabe einer explizite Einwilligung für das Profiling werden gesetzliche Vorgaben an Unternehmen gemacht, welche dazu führen, dass diese durch unnötige Bürokratie gebremst und jegliche Innovation verunmöglicht wird. Diese doch teils starken Verschärfungen die, wie bereits erwähnt, teilweise über das Ziel hinausschiessen („Swiss-Finish"), führen letztlich zu einer Restriktion genau der Unternehmen, welche die digitale Innovation vorantreiben und so den Bund in seiner Digitalen Strategie unterstützen. Diese Unternehmen und ihre Tätigkeit sind Quelle und Chance von neuen, innovativen, digitalen Geschäftsmodellen. Diesen Bereich so einzuschränken, würde nicht nur die Existenz von solchen Unternehmen gefährden, sondern führt dazu, dass man die digitale Entwicklung unnötig bremst oder sogar in extremis nicht mehr nutzen kann. Dies würde letztlich ein Widerspruch zur Digitalen Strategie des Bundes darstellen und den innovativen Wirtschaftsstandort Schweiz unnötig bremsen, was nicht im Sinne des Gesetzgebers gewesen sein kann.

	4. Einschränkung der Tätigkeit der Schweizer Medienschaffenden Der VE-DSG enthält in Art. 22 eine zum aktuellen Art. 10 DSG analoge Bestimmung über die „Einschränkung des Auskunftsrechts für Medienschaffende“. Zudem sieht Art. 24 Abs. 2 lit. d VE-DSG einen Art. 13. Abs. 2 lit. d entsprechenden Rechtfertigungsgrund für Medienschaffende vor. Damit wird das sogenannte „Medienprivileg“ aus dem aktuellen Recht übernommen. Der erläuternde Bericht hält denn in Ziff. 8.1.4.1 in Zusammenhang mit dem Auskunftsrecht auch fest, dass das sogenannte „Medienprivileg“ „keine materiellen Änderungen“ erfahren soll. Diese Klarstellung und Bestätigung ist zu begrüssen. Dennoch bergen einige der neuen Normen im VE-DSG die potentielle Gefahr, dass insbesondere die journalistische Arbeit der Medienschaffenden – und damit ihrer Kerntätigkeit – nur noch unter erschwerten Bedingungen möglich sein wird. Aufgrund der Tatsache, dass im VE-DSG – mit Ausnahme des Art. 22 VE-DSG, der für das Auskunftsrecht gilt – an keiner Stelle im Gesetz gesagt wird, dass insbesondere die Artt. 4 Abs. 5 u. 6a E (letzterer in Bezug auf Profiling), 12, 13, 15 (in Bezug auf Profiling), 16, 17, 19 lit. b, 25 Abs. 1 lit. c, 25 Abs. 2 , Art. 41 ff. VE-DSG nicht für Medienschaffende gelten, könnte auf eine Erweiterung des Anwendungsbereichs des VE-DSG geschlossen werden. Diese Annahme verstärkt sich denn auch dadurch, dass nicht wie bisher in Art. 10 DSG auf den Begriff „Datensammlung“ abgestellt wird, sondern zukünftig nunmehr auf den Begriff „Personendaten“ abgestellt werden soll. Diese hätte zur Folge, dass der VE-DSG in einem Ausmass auf die Tätigkeit der Schweizer Medienschaffenden anwendbar ist wie bisher nicht bzw. das Medienprivileg teilweise ausgehebelt werden würde. Das hätte unbestritten teilweise sehr weitreichende Folgen (s. Ausführungen unten, insbesondere zu Artt. 2, 22 und 24) und würde denn auch den verfassungsrechtlichen verankerten Informationsauftrag der Medien untergraben, was nicht gewollt sein kann. Die Arbeit mit der die Aufgabe der Medienschaffenden erfüllt wird, besteht hauptsächlich darin, Informationen und eben auch Personendaten zu erheben, zu bearbeiten und zu veröffentlichen. Die neuen Auflagen, welche das VE-DSG vorgibt, erschweren diese Tätigkeit erheblich (s. Ausführungen unten, insbesondere zu Artt. 2, 22 und 24). Dies kann für den Journalismus letztlich auch bedeuten, dass dieser nicht mehr ausgeübt werden kann. Erschwert wird hauptsächlich die journalistische Arbeit an sich (welcher Journalist wird bei jeder Recherche von jeder involvierten Person deren Einwilligung einholen können), aber auch die Finanzierung dieser Arbeit über Werbung sowie über den Nutzermarkt wird bei fehlenden Marketinglösungen zunehmend schwierig. Analyse- und Marketing-Möglichkeiten moderner Online-Medien werden oftmals stark kritisiert, aber dabei wird vergessen, dass marketing- und werbefinanzierte Inhalte inzwischen ein zentrales Standbein der Medienwelt geworden sind. Wer diese Möglichkeiten einschränkt, beschneidet damit die Medien in ihrer Tätigkeit genauso, wie wenn er ihnen inhaltliche Beschränkungen auferlegt. Es wäre deshalb zu begrüssen, wenn Rechtssicherheit bezüglich der Vorgaben an die Schweizer Medienschaffenden geschaffen werden würde.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
RIN	VE-DSG	2			Gemäss dem geltenden DSG sind die Medienschaffenden namentlich im Art. 10 und 13 Abs. 2 lit. d praktisch von der Geltung des DSG ausgenommen. Es sind denn auch nur ganz wenige Fälle bekannt, in denen in rechtlichen Auseinandersetzungen das DSG eine entscheidende Rolle gespielt hätte. Wenn es zu Prozessen kam, dann in der Regel gestützt auf den Persönlichkeitsschutz des ZGB (allenfalls UWG), aber eigentlich nie aufgrund des DSG (vgl. hierzu auch Amtl. Bull. SR 1990 Bd. 1-3 S. 128). Aufgrund der Tatsache, dass im VE-DSG – mit Ausnahme des Art. 22 VE-DSG, der für das Auskunftsrecht gilt – an keiner Stelle gesagt wird, dass insbesondere die Artt. 4 Abs. 5 u. 6a E (letzterer in Bezug auf Profiling), 12, 13, 15 (in Bezug auf Profiling), 16, 17, 19 lit. b, 25 Abs. 1 lit. c, 25 Abs. 2 , Art. 41 ff. VE-DSG nicht für Medienschaffende gelten, könnte auf eine systematische Veränderung durch den VE-DSG geschlossen werden und insbesondere auf eine Aushebelung des Medienprivilegs (s. Bemerkungen zu Art. 22 unten). Eine Klärung dieser eventuellen Rechtsunsicherheit würde sehr begrüsst werden. Es wäre opportun, die heute faktisch bestehende Grenzziehung zwischen Anwendungsbereich DSG und ZGB bereits in Art. 2 festzuhalten, so z.B. mit folgender (zu vervollständigen Formulierung): „Auf redaktionelle Beiträge in periodisch erscheinenden Medien ist das DSG nicht anwendbar.“
RIN	VE-DSG	2	3		Der Begriff „eidgenössische Gerichte“ bezeichnet Gerichte auf Bundesebene. Im Umkehrschluss sind alle kantonalen Gerichte nicht gemeint, also auch nicht vom Geltungsbereich des DSG ausgenommen. Das war aber bisher der Fall, weil im DSG von „Verfahren“ und nicht – wie neu – von Gerichten die Rede war. Der vorliegende Entwurfstext führt zu einer massiven Rechtsänderung. Es muss eine Präzisierung stattfinden, dass die Nichtunterstellung alle schweizerischen Gerichte erfasst, unabhängig von der Instanz und Benennung.
RIN	VE-DSG	3			Eines der Ziele der Revision des DSG war die Annäherung an die technischen Standards. Trotzdem haben gewisse grundlegende technische Definitionen, welche in der Praxis eine grosse Rolle spielen, keinen Eingang in den VE-DSG gefunden, insbesondere nicht die Begriffe „Daten“ (im technischen Sinn), „Anonymisierung“ und „Pseudonymisierung“. Gerade die präzise Abgrenzung von „Daten“ und „Personendaten“ würde in der Praxis sehr viel Rechtssicherheit schaffen. Auch die Definition der Begriffe

					„Anonymisierung“ und „Pseudonymisierung“ würde viele Unklarheiten beseitigen, zumal denn auch eine klare Abgrenzung der beiden Begriffe möglich wäre. Es ist unbestritten, dass die technischen Möglichkeiten, um z.B. Personendaten zu anonymisieren, sich immer weiter entwickeln, dennoch wäre es von Vorteil für die praktische Umsetzung des VE-DSG und die weiteren Vorgaben im VE-DSG, welche sich auf die Definitionen von „Personendaten“, „Daten“, „Anonymisierung“ und „Pseudonymisierung“ beziehen (z.B. „Profiling“), wenn eine klare, technologieneutrale Definition von diesen Begriffen bestehen würde. Es wird deshalb empfohlen, klare und technologieneutrale Definitionen unter Beiziehung von Fachpersonen aus der Praxis in den Begriffskatalog aufzunehmen. Des Weiteren wird empfohlen folgende Begriffe in den Definitionskatalog aufzunehmen: Empfänger, wesentliche persönliche Merkmale (Art. 3 lit. f VE-DSG), ausdrückliche Einwilligung (Art. 4 Abs. 6 VE-DSG).
RIN	VE-DSG	3	a		Es ist grundsätzlich zu begrüssen, dass die Definition von Personendaten beibehalten werden soll. Gilt denn so auch in der Schweiz weiterhin die bundesgerichtlich bestätigte relative Methode, welche besagt, dass es nicht ausreicht, dass der Aufwand zur Identifizierung objektiv gering genug ist, dass jemand ihn nach allgemeiner Lebenserfahrung auf sich nimmt. Es ist ebenso wesentlich, welches Interesse der Datenbearbeiter oder ein Dritter mit Zugang zu den Daten an der Identifizierung hat. So gilt nach wie vor die Einzelfallbeurteilung. Liest man den erläuternden Bericht, stellt man allerdings fest, dass der Inhalt des Begriffs „Personendaten“ doch geändert bzw. erweitert wird. Die vorgeschlagenen Änderungen sind jedoch teilweise unklar und widersprüchlich und schaffen keine klare Abgrenzung der Begriffe „Daten“ und „Personendaten“, im Gegenteil. Hinzu kommt, dass auch hier die in der Praxis sehr relevante Unterscheidung der „Anonymisierung“ von der „Pseudonymisierung“ nicht berücksichtigt wird. Gewisse Angaben, welche im erläuternden Bericht als „Personendaten“ definiert werden, sind in der Praxis von Beginn an als anonym einzustufen (definitiv nicht rückführbar) und deshalb ganz klar nur als „Daten“ einzustufen. Es wäre deshalb wünschenswert, dass eine klare Abgrenzung zwischen den Begriffen „Daten“ und „Personendaten“ sowie „Anonymisierung“ und „Pseudonymisierung“ gemacht werden (s. oben). Hinzu kommt, dass im erläuternden Bericht eine natürliche Person als bestimmbar erklärt wird, wenn sie

					„über Hinweise auf ihren Namen, eine Identifikationsnummer, Standortdaten, eine Online-Identität“ identifiziert werden kann. Diese Formulierung ist unpräzise und lässt sehr viel Raum für teilweise widersprüchliche Interpretationen, welche letztlich für den Bereich der Online-Aktivitäten (Werbung etc.) grosse Rechtunsicherheit schaffen. Unter dem geltenden DSG genügt es nicht, wenn Angaben bloss einer bestimmten „eindeutigen Kennung“ oder „Identifikationsnummer“, wie z.B. einer IP-Adresse, einer E-Mail-Adresse oder einer Cookie-Kennung, zugeordnet werden können, wenn die dahinterstehende Person nicht namentlich identifiziert werden kann (eine E-Mail-Adresse enthält zwar vielleicht einen Namen, ob der jedoch ein Pseudonym ist oder nicht, kann nicht verifiziert werden). Bei der Qualifikation dieser „Kennungs- oder Identifikationsnummern“ muss auch zukünftig **eine Einzelfallbeurteilung** möglich und entscheidend sein. Dies unter Berücksichtigung des Aufwands zur Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektiv) sowie ob überhaupt ein Interesse an der Identifizierung (subjektiv) besteht. So ist beispielsweise die namentliche Identifikation des Nutzers nicht von Interesse beim Einsatz von Cookies zur Bereitstellung von individualisierter Werbung (hier wird regelmässig auch die IP-Adresse mitbearbeitet). Hier findet lediglich eine Segmentierung statt und es besteht kein Interesse die einzelne Person zu identifizieren. Würde man zukünftig davon ausgehen, dass es sich bei diesen Kennungs- oder Identifikationsnummern immer um Personendaten handelt, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten. Viele unentgeltliche Angebote, welche durch Werbung finanziert werden, würden künftig der Allgemeinheit nicht mehr zur Verfügung stehen. Es ist deshalb wichtig im erläuternden Bericht klarzustellen, dass der Einzelfall und somit das subjektive Interesse an der Identifizierung beurteilt werden soll und nicht darauf abgestellt werden kann, ob es objektiv möglich ist oder irgendwann möglich sein wird, die hinter den Kennungs- oder Identifikationsnummern stehende Person zu identifizieren.
RIN	VE-DSG	3		c.4	Die Begriffe „biometrische Daten“ sowie „spezifische, technische Mittel“ müssen präzisiert werden. Die Beschreibung im erläuternden Bericht lässt darauf schliessen, dass Fotos, welche in den Medien veröffentlicht und dafür mit spezifischen, technischen Mitteln so bearbeitet werden, dass eine eindeutige Identifizierung oder Authentisierung einer Person möglich ist, immer ein biometrisches Datum sind. Es ist nicht klar, was mit „spezifischen technischen Mitteln“ gemeint ist. Fotos werden in der Praxis immer bearbeitet und dienen in den meisten Fällen der Identifizierung, gelegentlich werden sie aber auch gerade zur Verhinderung einer solchen bearbeitet (Balken, Verpixelung). Es kann nicht angehen, dass in solchen Fällen immer von einem biometrischen Datum ausgegangen werden muss.

RIN	VE-DSG	3		e	Die Definition von „Bekanntgeben“ enthält neu den Begriff „Übermitteln“. Im erläuternden Bericht wird jedoch nicht darauf eingegangen oder wenigstens umschrieben, was damit genau gemeint ist. Erfasst der Begriff das „Übermitteln an Dritte“ ausserhalb des eigenen Unternehmens oder bereits das Übermitteln innerhalb desselben Unternehmens gemeint? Hinzu kommt, dass nicht jedes Übermitteln bereits eine Bekanntgabe im Sinn von Zugänglichmachen von Personendaten ist. Eine Präzisierung hinsichtlich der Definition des Begriffs und das Erläutern der Beweggründe im erläuternden Bericht wären wünschenwert.
RIN	VE-DSG	3		f	Die vorgeschlagene Definition des Profilings und die damit einhergehende Regelung der ausdrücklichen Einwilligung (s. Art. 23 VE-DSG, unten) ist aus verschiedenen Gründen abzulehnen: Die Definition geht unbegründet weit über diejenige der EU-DSGVO hinaus (Art. 4 Ziff. 4). In der E-SEV 108 gibt es keine Vorgaben für das Profiling. Es wird nur eine Regelung für die automatisierten Entscheidungen (vgl. Art. 8 Abs. 1 lit. a) verlangt. Es sind somit keine Beweggründe zu erkennen, welche zu einer derartig weitgehenden Definition des Profilings in der Schweiz führen sollten. Es sollte deshalb davon abgesehen werden, Schweiz-spezifische Vorgaben für das Profiling zu machen. Rein schon nur der Schritt vom „Persönlichkeitsprofil“ (statischer Ausdruck) zu Profiling (dynamischer Begriff) bedeutet in der Praxis eine grosse Umstellung und wirft viele Fragen und damit Rechtsunsicherheiten auf. Wenn überhaupt, muss das Profiling zwingend auf automatisierte Bearbeitungen beschränkt bleiben. Der Begriff „wesentliche persönliche Merkmale“ ist näher zu definieren. Die Rechtsunsicherheit in der Praxis bezüglich der konkreten Definition von „Persönlichkeitsprofil“ sollte behoben werden und nicht dahingehend weiter geführt werden müssen, als dieselben Diskussionen nun in Bezug auf die Definition von „wesentliche persönliche Merkmale“ geführt werden müssen. Die aufgeführten Begriffe „Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre und Mobilität“ sind sehr unspezifisch und lassen deshalb sehr viel Raum für Interpretationen. Wünschenswert wäre ein Katalog in der zukünftigen VDSG, welche Aspekte im jeweiligen Bereich denn konkret davon erfasst werden. Eine allfällige Regelung sollte zudem nicht so weit gefasst sein, dass sie sogar für das Profiling mit nicht personenbezogenen Daten gilt. Der Passus „von Daten oder“ ist deshalb ersatzlos zu streichen. Eine Aussage wie im erläuternden Bericht (S. 44), dass alle beim Profiling entstehenden Daten grundsätzlich Personendaten sind, ist nicht korrekt, da in der Realität das Gegenteil der Fall ist. Es ist deshalb, wie oben erwähnt (s. Kommentar zu Art. 3 VE-DSG), unerlässlich Definitionen bestimmter, technischer, in der

					praktischen Umsetzung des DSG relevanter Ausdrücke festzuhalten. Hinzu kommt, dass für die im erläuternden Bericht angesprochenen Bearbeitungen (Analysen im Rahmen von Big Data) die übrigen Regelungen bereits vollumfänglich genügen. Darüber hinaus wird die Unsicherheit, welche konkreten Bearbeitungen in der Praxis als Profiling zu betrachten sind, durch den Passus „von Daten oder“ weiter verstärkt.
RIN	VE-DSG	4	3		Es wird begrüsst, dass Personendaten neu auch für Zwecke verwendet werden dürfen, die mit dem ursprünglichen Zweck kompatibel sind. Es sollte in der Botschaft betont werden, dass dies auch die Nutzung und Weitergabe von Daten innerhalb von Gruppengesellschaften ermöglicht. „Klar“ ist zu streichen. Es schafft Interpretationsspielraum und damit Rechtsunsicherheit. Da gemäss dem erläuternden Bericht die geltende Rechtslage zu ändern nicht beabsichtigt und auch nicht erforderlich ist, sorgt diese Neuformulierung nur für Unsicherheit.
RIN	VE-DSG	4	4		Diese lit. ist zu streichen. Der Inhalt ergibt sich bereits aus dem Verhältnismässigkeitsprinzip.
RIN	VE-DSG	4	5		Der heutige Wortlaut (Art. 5 Abs. 1 DSG) soll beibehalten werden. Gemäss dem erläuternden Bericht soll keine materielle Änderung der Rechtslage erfolgen. Dann muss auch der Wortlaut unverändert bleiben. Zumal die neue Formulierung dazu führen würde, dass man Personendaten, welche man aus verschiedenen Gründen aufbewahrt („Aufbewahren“ wird auch als „Bearbeiten“ definiert, s. Begriffsdefinitionen Art. 3 lit. d VE-DSG) oder gar aus gesetzlichen Gründen aufbewahren muss, wenn nötig nachführen müsste. Es ist nicht klar, was mit „wenn nötig“ gemeint ist, wenn es sich um das Aufbewahren von Personendaten handelt, und eine Verpflichtung zur permanenten Nachführung wäre schlichtweg nicht erfüllbar und ist im Fall der blossen Aufbewahrung alter Daten auch nicht nötig.
RIN	VE-DSG	4	6		Der neue Wortlaut bzw. das Einfügen des Wortes „eindeutig“ schafft Rechtsunsicherheit, zumal es im erläuternden Bericht nicht definiert wird. Es ist unklar, ob mit der terminologischen Anpassung an die DSGVO auch eine materielle Änderung vollzogen wird. Die Definition dieses Begriffs ist insbesondere für die praktische Umsetzung in der Werbebranche von grosser Bedeutung und würde für grosse Rechtssicherheit sorgen. Für weitere Unsicherheit bezüglich die praktische Umsetzung insbesondere im Hinblick auf das Profiling

					(s. unten) sorgen die Ausführungen im erläuternden Bericht zur „ausdrücklichen" Einwilligung. Es ist nicht klar, welche Bedingungen erfüllt sein müssen, damit eine ausdrückliche Einwilligung vorliegt: Sind es dieselben wie im geltenden Recht, oder gibt es neue Auflagen? Dies stellt insbesondere in der Werbebranche ein Problem dar und muss eindeutig im Gesetz geklärt werden.
RIN	VE-DSG	7	3		Dieser Absatz ist ersatzlos zu streichen. Eine zwingende Zustimmung zum Beizug von Sub-Auftragsdatenbearbeitern ist weder durch die internationalen Verpflichtungen gefordert noch entspricht sie der geltenden Rechtslage in der Schweiz. Hinzu kommt, dass sie in der Praxis nicht umsetzbar wäre. Die Bestimmung muss zumindest dahingehend angepasst werden, dass nicht „Schriftlichkeit" erforderlich ist, sondern eine Form, die den Nachweis durch Text ermöglicht. Andernfalls wäre die Ermächtigung zur Einsetzung von Unterauftragnehmern namentlich in Verträgen, die online abgeschlossen werden, nicht mehr möglich.
RIN	VE-DSG	8			Die Schaffung von Empfehlungen der guten Praxis wird sehr begrüsst. So stellen sie doch die der wirtschaftsliberalen Schweiz inhärente Selbstregulierung in den Vordergrund. Es besteht jedoch Klärungsbedarf hinsichtlich der interessierten Kreise, der Verbindlichkeit dieser Empfehlungen sowie allfälliger Rechtsmittel gegen diese. In Frage gestellt wird auch, ob es überhaupt in das Aufgabengebiet einer Aufsichtsbehörde fällt, die Kompetenz zu erhalten, solche Empfehlungen der guten Praxis zu erlassen. Es wäre sinnvoller, wenn diese in der jeweiligen Branche erstellt werden würden.
RIN	VE-DSG	8	1		Sollte die Kompetenz des EDÖB zum Erlass der Empfehlungen der guten Praxis bestehen bleiben, ist diese insofern problematisch, als nicht klar ist, ob es sich dabei um Verfügungen handelt und diese angefochten werden können. Hinzu kommt, dass trotz der Klarstellung in Art. 9 Abs. 3 VE-DSG deren Verbindlichkeit nicht klar ist. Es wäre wünschenswert, wenn die interessierten Kreise näher bezeichnet werden würden und auch festgelegt würde, nach welchen Kriterien der EDÖB diese beizieht. Des Weiteren müsste geklärt werden, ob interessierte Kreise die Verbände mit einschliesst oder diese gerade exkludiert. Sicherzustellen ist, dass die Interessen nicht verbandsangehöriger Unternehmen berücksichtigt werden, insbesondere wenn sie denjenigen des Verbandes ihrer Branche zuwiderlaufen. Eine weitere Frage ist die nach der Berücksichtigung der Konkurrenzverhältnisse der interessierten Kreise innerhalb derselben Branche. Soll eine Empfehlung der guten Praxis des einen Konkurrenten, welche vom EDÖB für verbindlich erklärt

					wurde, für den anderen Konkurrenten gelten, auch wenn er damit nicht einverstanden ist? Hat er ein Rechtsmittel dagegen?
RIN	VE-DSG	8	2		Hinsichtlich des Genehmigungsverfahrens durch den EDÖB stellt sich die Frage, ob er die richtige Instanz ist oder noch eine weitere beigezogen werden sollte. Der EDÖB hat nur sehr beschränkte personelle Ressourcen. Die Genehmigung der vorgelegten Empfehlungen der guten Praxis würde unter den jetzt gegebenen Verhältnissen entweder lange dauern oder gezwungenermassen nur oberflächlich erfolgen. Letzteres würde die „Best Practices“ gleich zur reinen Alibiübung deklassieren.
RIN	VE-DSG	8	3		Faktisch dürften diese Empfehlungen einen über die gesetzlichen Vorgaben hinausgehenden Standard setzen, der nach Veröffentlichung durch den EDÖB als verbindlich betrachtet wird. Im Hinblick darauf, dass sich sogar Gerichte in ihrer Rechtsprechung am EDÖB bzw. den Informationen auf seiner Seite orientieren, ist der gesetzesgleiche Status von nicht zu unterschätzender Bedeutung, aber auch rechtsstaatlicher Problematik.
RIN	VE-DSG	13	1		Die Informationspflicht wird auf alle Personendaten ausgeweitet, was zu erheblichem Mehraufwand für die Unternehmen führen wird. Unklar ist ferner, inwiefern die Informationspflicht auch gilt, wenn nachträglich neue Bearbeitungszwecke hinzukommen oder andere Bearbeitungen an die Stelle der ursprünglichen treten. Diesbezüglich ist eine Klarstellung erforderlich, dass nur über das informiert werden muss, was schon zum Zeitpunkt der Beschaffung feststand. Zudem muss zwingend klargestellt werden, dass – entsprechend der geltenden Rechtslage und der Praxis des EDÖB – bei der Beschaffung grundsätzlich ein Verweis auf die auf einer Website enthaltenen Detailinformationen ausreicht. Die Erwägung im erläuternden Bericht, wonach es nicht genügt, wenn die betroffene Person nach den Informationen suchen muss, ist abzulehnen.
RIN	VE-DSG	13	2		Hinsichtlich des Zeitpunkts der Information ist für den Online-Kontext eine Klarstellung erforderlich. Denn beim Zugriff auf eine Website wird regelmässig eine Bearbeitung von IP-Adressen erfolgen (Erfassung in Log-Datei, Zählung der Website-Zugriffe etc.), und dies in der Regel bereits *bevor* der Nutzer allfällige Informationen hierzu z.B. in einer Datenschutzerklärung zur Kenntnis nehmen kann. Aufgrund der Tatsache, dass IP-Adressen - je nach Einzelfall - Personendaten darstellen können, und dass eine vorgängige Information hier technisch grundsätzlich nicht möglich ist, muss klargestellt werden, dass die

					ausreichend kenntlich gemachte Information in einer Datenschutzerklärung auch noch *nach* Abruf der Website als rechtzeitig gilt. Hinsichtlich des Zeitpunkts der Information ist auch für die journalistische Tätigkeit eine Klarstellung erforderlich. Ist mit Beschaffung der Zeitpunkt der Recherchearbeit, der Speicherung oder der Veröffentlichung des daraus resultierenden Artikels im Medium gemeint? Was gilt, wenn ein Journalist im eigenen Medienarchiv recherchiert? Präzision bezüglich aller offenen Punkte wird gewünscht. Im Hinblick darauf, dass das Nichterfüllen der Informationspflichten mit Sanktionen bedroht wird, muss eine abschliessende Aufzählung der mitzuteilenden Informationen erfolgen (strafrechtliches Bestimmtheitsgebot). Andernfalls würden sich Unternehmen zur Vermeidung von Risiken dazu gezwungen sehen, den betroffenen Personen eine Vielzahl der Informationen, wie sie in der EU-DSGVO vorgesehen sind, mitzuteilen. Ein Übermass an Information bewirkt aber das Gegenteil von Aufklärung, nämlich systematische Überforderung und routinemässiges Desinteresse an den Inhalten. Sie führt nicht zu mehr, sondern im Ergebnis zu weniger Transparenz.
RIN	VE-DSG	13	4		Diese Bestimmung geht weit über die DSGVO hinaus und ist abzulehnen. Diese Vorschrift führt zu einer weiteren Aufblähung von AGB und Datenschutzerklärungen, dadurch für die Unternehmen zu mehr Aufwand und vor allem zu einer Überflutung der betroffenen Personen mit weder nachgesuchten noch in der Regel verständlichen Informationen, welche in den meisten Fällen ohnehin nicht gelesen werden.
RIN	VE-DSG	13	5		Auch diese Regelung ist viel strenger als die Regelung in der DSGVO. Sie verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Unmittelbar nach der Beschaffung werden die Daten gespeichert und in der Regel erst nachher überhaupt gelesen. Diese praxisfremde Regelung sollte stattdessen durch eine Regelung in Anlehnung an die DSGVO ersetzt oder zumindest das „spätestens“ gestrichen werden.
RIN	VE-DSG	14	4	a	Der Katalog der Ausnahmen ist enger gefasst als es nach dem E-SEV 108 erforderlich wäre. So ist bspw. die Berufung auf ein überwiegendes Interesse nicht möglich, wenn die Daten einem Dritten weitergegeben werden (dies kann ja auch innerhalb eines Konzerns der Fall sein). Für diese Einschränkung gibt es keine plausible Erklärung. Sie ist deshalb zu streichen. Entweder ist ein überwiegendes Interesse des Verantwortlichen vorhanden oder nicht. Dies wird im Rahmen einer Interessenabwägung eruiert werden, hat aber letztlich Nichts mit einer Bekanntgabe an Dritte zu tun. Die

					vorgeschlagene Regelung würde bspw. dazu führen, dass Journalisten künftig keine Recherchen mehr durchführen könnten, ohne nicht jede einzelne Person, über die sie Daten erhalten, darüber zu informieren, denn die Journalisten könnten sich nicht auf die Ausnahmeregelung beziehen, da sie die Informationen in der Regel in den Medien an Dritte weitergeben.
RIN	VE-DSG	15			Der Anwendungsbereich der Informations- und Anhörungspflicht ist viel zu weit gefasst, da gemäss den Erläuterungen bereits „beliebige rechtliche Wirkungen" genügen. Es muss daher zumindest vorausgesetzt werden, dass die rechtlichen Auswirkungen eines Einzelentscheids eine gewisse Schwere erreichen. Hinzu kommt, dass diese Regelung zu den automatisierten Einzelfallentscheidungen über die Vorgaben der DSGVO hinausgeht und auch gemäss dem E-SEV eine derart strenge Regelung nicht vorgesehen ist. Dieser Artikel ist deshalb entsprechend anzupassen.
RIN	VE-DSG	16			Diese Regelung muss aus verschiedenen Gründen angepasst werden, insbesondere weil es sich im Vergleich zur EU-Datenschutzgesetzgebung um eine weitere Schweizer Verschärfung handelt (Swiss Finish). Erneut sind auch die Begrifflichkeiten vage und lassen viel zu viel Spielraum für Interpretationen, was letztlich wieder zu Rechtsunsicherheit führt.
RIN	VE-DSG	16	1		Die Definition von „voraussichtlich", „erhöhtes Risiko" sowie „vorgängig" fehlt. Insbesondere das „erhöhte Risiko" lässt zuviel Spielraum für Interpretationen zu. Hinzu kommt, dass die Anknüpfung an das Vorliegen „erhöhter Risiken" zu einem viel zu weit gefassten Anwendungsbereich führt und – ein weiteres Swiss Finish - unverständlicherweise über die Vorgaben in der EU-DSGVO (Art. 35) hinaus geht .Der Entwurf und die Erläuterungen geben keine Klarheit darüber, was ein „erhöhtes Risiko" sein soll. Jedes noch so kleine Risiko kann als „erhöht" gegenüber „keinem Risiko" angesehen werden. Diese Formulierung ist zu streichen. Bleibt es bei dieser Formulierung, würde diese zu einem übermässigen Aufwand führen, der sowohl für die Unternehmen als auch für den EDÖB nicht zu bewältigen ist. Denn ausgehend von einem „erhöhten Risiko", könnte eine solche Pflicht zur Datenschutz-Folgeabschätzung letztlich bei jeder Übermittlung in Länder wie die USA, jedem Profiling und jeder Bearbeitung von besonders schützenswerten Daten bestehen, die voraussichtlich zu einer Datenschutzverletzung führen könnten. Dies würde insbesondere für die Unternehmen, welche personalisierte Werbung und Tracking anwenden zu massiven Kosten führen, da die Pflicht bspw. auch für das Profiling zur Einblendung personalisierter Werbung oder beim Web-Tracking bestehen würde. Des Weiteren würde auch eine

					Datenschutz-Folgeabschätzung für jeden journalistischen Artikel erstellt werden müssen, stellt doch jedes Verfassen eines Artikels über eine Person voraussichtlich ein erhöhtes Risiko einer Persönlichkeitsverletzung dieser Person dar oder gar eine Gefährdung ihrer Grundrechte. Die Umsetzung der vorgeschlagenen Formulierung in der Praxis dürfte weder erwünscht noch möglich sein. Entsprechend der EU-Regelung sollte daher nur auf Datenbearbeitungen mit „hohem Risiko“ (oder besser „besonders hohem Risiko“) abgestellt werden. Dabei sollten auch diejenigen Fälle, in denen die Pflicht besteht, (zumindest beispielhaft) konkretisiert und Ausnahmen vorgesehen werden. Ausgenommen werden sollten namentlich Fälle, in welchen die Betroffenen mit den Datenbearbeitungen einverstanden sind oder bereits eine Ausnahme bestand. Des Weiteren ist die Bezugnahme auf die Risiken für die „Grundrechte“ von Betroffenen bei Datenbearbeitungen durch Private unpassend und folglich zu streichen. Die vorgeschlagene Regelung geht sodann auch in weiteren Punkten über die EU-DSGVO hinaus (Swiss Finish): So ist die Pflicht entsprechend der EU-Vorschriften (Art. 35 DSGVO) auf den Verantwortlichen zu beschränkten. Eine Ausdehnung auf den Auftragsdatenbearbeiter ist nicht nachvollziehbar und ergibt letztlich keinen Sinn.
RIN	VE-DSG	16	3		Im Hinblick darauf, dass bei *jeder* auch bloss vorgesehenen Datenbearbeitung, welche voraussichtlich zu einem erhöhten Risiko führen kann, eine Datenschutz-Folgeabschätzung durchgeführt und diese mit dem Resultat und den vorgesehenen Massnahmen dem EDÖB eingereicht werden muss, ist die Meldepflicht viel zu weit gefasst. Abgesehen davon, dass es zu einer Aufblähung der Bürokratie innerhalb der Unternehmen führen würde, wäre die Menge der eingereichten Datenschutz-Folgeabschätzungen, derart gross, dass der EDÖB sie unmöglich bewältigen könnte. Es ist somit, wenn überhaupt, nur dann eine Meldepflicht gegenüber dem EDÖB vorzusehen, wenn trotz der getroffenen Schutzvorkehrungen nach Auffassung des Verantwortlichen nach wie vor ein „hohes Risiko“ einer Datenschutzverletzung besteht. Mehr verlangt auch die EU-DSGVO nicht (Art. 36 Abs. 1).
RIN	VE-DSG	16	4		Die Frist von drei Monaten zur Beurteilung durch den EDÖB ist länger als diejenige in der EU-DSGVO (Art. 36 Abs. 2). Das Abwarten dieser Frist ist im Hinblick darauf, dass für jede Datenbearbeitung, die voraussichtlich zu einem erhöhten Risiko führen kann, eine Datenschutz-Folgeabschätzung durchgeführt werden muss, nicht praktikabel und führt zu einer erheblichen Einschränkung der Handlungsfreiheit der

					Unternehmen und letztlich zu einer Lähmung der Wirtschaft. Die Frist muss daher erheblich verkürzt werden.
RIN	VE-DSG	17			Nach dieser Regelung besteht gegenüber dem EDÖB grundsätzlich für *jede* „unbefugte Datenbearbeitung“ oder „den Verlust von Daten“ eine „unverzügliche“ Meldepflicht. Es hat somit bei jedem noch so geringfügigen Verstoss eine Meldung zu erfolgen, selbst wenn dieser voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt. Die vorgesehene Regelung geht viel zu weit („jede unbefugte Datenbearbeitung“) und führt auch nicht dazu, dass der Schutz der Betroffenen letztlich höher ist. Denn eine entsprechende Meldung an die betroffene Person wird ja gemäss Abs. 2 nur dann gemacht, wenn es zum Schutz der der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. Wird diese Regelung so umgesetzt wie sie im VE-DSG steht, würde es dazu führen, dass enorm weitfassende innerbetriebliche Kontrollmassnahmen aufgebaut werden müssten, die letztlich zu einer permanenten Mitarbeiterüberwachung führen würden: Anders kann ja gar nicht sichergestellt werden , dass jede unbefugte Datenbearbeitung oder jeder mögliche Verlust von Daten unverzüglich gemeldet werden kann. Inwiefern eine solches innerbetriebliches Kontrollsystem mit dem arbeitsrechtlich verankerten Verbot der ständigen Mitarbeiterüberwachung zu vereinbaren ist, sei dahingestellt (vgl. Art. 26 Arbeitsverordnung 3). Hinzu kommt, dass die Begrenzung des Anwendungsbereichs viel zu vage ist. „Voraussichtlich“ lässt viel Raum für (richterliche) Interpretation zu und führt zu Rechtsunsicherheit und letztlich zu einer Flut an Meldungen, welche weder auf Seiten der Unternehmen noch auf Seite des EDÖB zu bewältigen sein wird. Hinzu kommt, dass hiermit eine weitere Regelung vorliegt, welche weiter geht als die Regelung im E-SEV (Art. 7 Abs. 2). Entsprechend ist diese Regelung anzupassen. So ist die Meldepflicht auf Verletzungen zu beschränken, welche die Rechte der Betroffenen „schwerwiegend“ gefährden könnten. Es ist überdies zu definieren, in welcher Zeitspanne solche Meldungen zu erfolgen haben und in welchen Fällen eine Meldung unabhängig von der Stellungnahme des EDÖB an die betroffen Person zu erfolgen hat. Hängt die Mitteilung an die betroffene Person nämlich von der Beurteilung des EDÖB ab, könnte die Flut der Meldungen an den EDÖB dazu führen, dass die betroffene Person sehr viel später von der unbefugten Datenbearbeitung erfährt, als dies die vorliegende Regelung erreichen möchte.
RIN	VE-DSG	18			Die Einführung dieser neuen Vorgaben - Privacy by Default und Privacy by Design ist problematisch, zumal die Nichteinhaltung mit Sanktionen bedacht ist. Es gibt bei beiden nicht die eine richtige

					Vorgehensweise, ein gewisser Spielraum in der Ausgestaltung muss den Anwendern deshalb eingeräumt werden. „Angemessene Massnahmen“ und „geeignete Voreinstellungen“ sind daher als auslegungsfähig und anpassungsfähig an die technischen Gegebenheiten einzustufen. Dies geht nicht aus dem erläuternden Bericht hervor und muss deshalb festgehalten werden. Abgesehen davon ist die Sanktionierung insbesondere auch mit Blick auf das strafrechtliche Bestimmtheitsgebot problematisch.
RIN	VE-DSG	19		a	Die vorgeschlagene Dokumentationspflicht ist zu weit gefasst und führt für Unternehmen zu einem erheblichen und unnötigem Aufwand. Die Regelung darf keinesfalls über das in der EU-DSGVO (Art. 30) vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgehen. Damit ein solches Verzeichnis überhaupt seinen Zweck erfüllen kann, muss es jedenfalls auf regelmässige Datenbearbeitungen beschränkt sein, andernfalls müsste bereits jegliche Korrespondenz darin erfasst werden. Darüber hinaus sind, wie auch im Rahmen der EU-DSGVO (Art. 30 Abs. 5), entsprechende Ausnahmen vorzusehen. In der vorgesehenen Form ist diese Bestimmung ein unnötiges schweizerisches Überschiessen (Swiss Finish).
RIN	VE-DSG	19		b	Dieser Artikel ist hinsichtlich der Tatsache, dass die Informations- und Meldepflichten auf Personendaten (anstelle von Persönlichkeitsprofilen und besonders schützenswerte Personendaten) erweitert wurde und auch nicht mehr an eine Datensammlung gebunden ist, viel zu weit gefasst. Es ist aus grundsätzlichen Gründen dann auch ungenügend, wie aber im erläuternden Bericht festgehalten (S. 65), dass eine Konkretisierung der Angaben erst in der Verordnung stattfindet. Sämtliche Bearbeitungen von Personendaten zu dokumentieren führt selbstverständlich zu einem erhöhten bürokratischen Aufwand, dessen Mehrwert für die betroffene Person nicht erkennbar ist. Es muss deshalb eine Abwägung zwischen dem Aufwand der Unternehmen und den Interessen der betroffenen Personen vorgenommen werden, die keinen unverhältnismässigen Aufwand für die Unternehmen zur Folge hat.
RIN	VE-DSG	20	1		Die Kostenlosigkeit des Auskunftsrechts ist zu streichen. Sie entspricht nicht der heute geltenden Regelung im Schweizer Recht, gemäss der ausnahmsweise eine angemessene Beteiligung an den Kosten verlangt werden kann (vgl. Art. 2 VDSG); dies insbesondere, wenn die Auskunftserteilung mit einem besonders grossen Arbeitsaufwand verbunden ist. Es ist aber abzusehen, dass der Aufwand künftig, aufgrund der erhöhten Informationspflichten, grundsätzlich höher als jetzt sein wird. Hinzu kommt, dass die Kostenlosigkeit sich nicht aus dem E-SEV 108 ergibt. In Art. 8 Abs. 1 lit. b) E-SEV 108 wird nur

					verlangt, dass die Auskunftserteilung ohne übermässige Kosten zu erfolgen hat. Es muss somit weiterhin möglich sein, eine angemessene Aufwandsentschädigung zu verlangen, wenn gewisse Voraussetzungen eintreten. Mit Beibehaltung der Regelung gemäss Art. 2 VDSG wird auch in Zukunft einem Missbrauch des Auskunftsrechts vorgebeugt werden (Querulanten).
RIN	VE-DSG	20	3		Die vorgesehene Regelung würde für jede Datenbearbeitung gelten, aufgrund welcher eine Entscheidung gefällt wird. Die Formulierung ist damit viel zu weit gefasst und muss entsprechend eingeschränkt werden. Es handelt sich auch hier um ein weiteres, überschiessendes Swiss-Finish. Entsprechend der Regelung in der EU-DSGVO (Art. 15 Abs. 1 lit. h) ist das Auskunftsrecht auf diejenigen Fälle zu beschränken, in welchen auch eine Informations- und Anhörungspflicht nach Art. 15 VE-DSG besteht, also auf Entscheidungen, die automatisiert erfolgen und entsprechende Auswirkungen haben.
RIN	VE-DSG	22			Gemäss dem erläuternden Bericht soll sich durch die Übernahme des Art. 10 DSG in Art. 22 VE-DSG keine materiellen Änderungen ergeben. Dies ist zu begrüssen. Mit dem Verzicht auf den Begriff der „Datensammlung“, wie er in Art. 10 DSG enthalten ist, und dem Abstellen – neu - auf „Personendaten“ wird sich dennoch eine Rechtsänderung ergeben und dies wird sogar zu einer Ausdehnung des Geltungsbereichs des DSG führen. War bis anhin Anknüpfungspunkt der klar definierte Begriff „Datensammlung“, so wird jetzt alleine das „Bearbeiten von Personendaten“ massgebend sein. Nicht jedes Bearbeiten von Personendaten führt heute automatisch zur Entstehung einer Datensammlung, z.B. Personendaten, die bei einer Recherche oder einem Archivstudium bearbeitet wurden. Mit der neuen Formulierung werden alle diese Personendaten auch erfasst. Das ist weder sinnvoll noch zielführend, zumal solche Rechercheresultate oftmals sofort wieder gelöscht oder eben gerade nicht systematisch in einer Datensammlung abgelegt werden. Die vorgeschlagene Neuerung führt – entgegen den verkündeten Absichten – zu einer unnötigen Bürokratie. Das Ziel, den Bürger transparent darüber zu informieren welche Daten denn nun konkret bearbeitet werden, wird dadurch nicht erreicht, vor allem dann nicht, wenn blosse Recherchearbeit nicht verwertbares Material produziert. Hinzu kommt, dass Art. 22 VE-DSG nur die Einschränkung des Auskunftsrechts regelt und systematisch im Kapitel „Rechte der betroffenen Person“ angegliedert ist. Wohingegen Art. 10 DSG im Kapitel „Allgemeine Datenschutzbestimmungen“ angegliedert ist. Es ist deshalb nicht klar, wie diese neue systematische Einordung zu interpretieren ist. Zumal an keiner Stelle gesagt wird, dass insbesondere die Artt. 4 Abs. 5 u. 6a E (letzterer in Bezug auf Profiling), 12, 13, 15 (in Bezug auf Profiling), 16, 17, 19 lit. b,

					25 Abs. 1 lit. c, 25 Abs. 2 , Art. 41 ff. VE-DSG nicht für Medienschaffende gelten. Sind die Medienschaffenden im geltenden DSG namentlich im Art. 10 und 13 Abs. 2 lit. d praktisch von der Geltung des DSG ausgeschlossen gewesen, könnte aufgrund des VE-DSG auf eine systematische Veränderung geschlossen werden. Dies würde bedeuten, dass beispielsweise Art. 16 VE-DSG (Erstellen einer Datenschutz-Folgeabschätzung) auf die journalistische Tätigkeit Anwendung finden würde. Eine Klärung dieser Rechtsunsicherheit ist dringlich (s. Erläuterungen zu Art. 2 oben).
RIN	VE-DSG	23	1	d	Das Einstufen von Profiling als Persönlichkeitsverletzung per se ist zwingend zu streichen, insbesondere wenn man die momentan vorgesehene, viel zu weite Definition des Profilings im VE-DSG ansieht (s. Ausführungen zu Art. 3 lit. f oben). Hinzu kommt, dass das Erfordernis der ausdrücklichen Einwilligung für das Profiling, damit es als gerechtfertigt gilt, eine unverhältnismässig strenge Vorgabe ist, die weder im E-SEV 108 noch in der DSGVO verlangt wird. Werden die Datenbearbeitungsgrundsätze eingehalten, ist nicht nachvollziehbar, weshalb nebst der Information auch eine ausdrückliche Einwilligung erforderlich ist. Zumal denn auch in vielen Punkten nicht klar ist, wie die ausdrückliche Einwilligung in der Praxis umgesetzt werden soll. Insbesondere für die Werbebranche hat diese Anforderung erhebliche und ebenso unerwünschte wie unnötige Konsequenzen. Die Vorschrift erschwert oder verunmöglicht faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt letztlich eine Bedrohung für den Wirtschaftsstandort Schweiz dar. Profiling - und damit personalisierte Werbung - wäre dann faktisch nur noch den grossen (insbesondere internationalen) Giganten wie Facebook, Google, Apple und Co. vorbehalten, da sich diese Unternehmen meist problemlos auf eine entsprechende, ausdrückliche Einwilligung im Rahmen der Account-Registrierungen stützen können.
RIN	VE-DSG	24	2		Das Wort „möglicherweise“ ist zu streichen. Mit einer Aufzählung von Rechtfertigungsgründen, welche ein überwiegendes Interesse darstellen, soll Rechtssicherheit geschaffen werden. Die in keiner Weise begründete Neuformulierung führt weg von der relativen Sicherheit des geltenden Gesetzes.
RIN	VE-DSG	24	2	d	Art. 24 Abs. 2 lit. d VE-DSG sieht einen Art. 13. Abs. 2 lit. d entsprechenden Rechtfertigungsgrund für Medienschaffende vor. Damit wird das sogenannte „Medienprivileg“ aus dem aktuellen Recht übernommen. Der erläuternde Bericht hält denn in Ziff. 8.1.4.1 in Zusammenhang mit dem Auskunftsrecht auch fest, dass das sogenannte „Medienprivileg“ „keine materiellen Änderungen“ erfahren

					soll. Diese Klarstellung und Bestätigung ist zu begrüssen. Sie gilt auch für den Rechtfertigungsgrund gemäss Art. 24 Abs. lit. d VE-DSG. Nicht nachvollziehbar ist deshalb das hinzugefügte Wort „möglicherweise“. Es bezieht sich auf sämtliche der aufgezählten Rechtfertigungsgründe und damit auch auf denjenigen für die journalistischen Datenbearbeitungen. Die Änderung birgt das Risiko einer Relativierung des Medienprivilegs in der Praxis. Diese Änderung ist somit nicht nur nicht erforderlich, sondern sie stiftet vielmehr Verwirrung, Rechtsunsicherheit und gefährdet dadurch auch die journalistische Arbeit der Medienunternehmen. Das Wort „möglicherweise“ ist folglich zu streichen.
RIN	VE-DSG	44	3		Diese Regelung ist abzulehnen. Die Einstellung oder Anpassung von Datenbearbeitungen während der ungewiss langen Dauer des Verwaltungsverfahrens kann massive und durchaus auch irreparable Schäden für die Unternehmen verursachen. Den Betroffenen muss zumindest die Möglichkeit gegeben werden, die Erteilung der aufschiebenden Wirkung durch die zuständige Rechtsmittelinstanz zu beantragen.
RIN	VE-DSG	50-55			Die vorgesehenen Strafbestimmungen sind abzulehnen. Sie führen zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz befassten Mitarbeiter. Sie werden dazu führen, dass die gesetzlich gewollten Spielräume bei der Datenbearbeitung aus Angst vor persönlicher Bestrafung nicht ausgeschöpft werden und sehr viel mehr Bürokratie betrieben werden wird als sinnvoll. Statt sich auf die Einhaltung des Datenschutzes zu fokussieren (die Verletzung der Bearbeitungsgrundsätze wird nicht sanktioniert), werden alle Ressourcen auf die Einhaltung der formalen, mit Strafe bedrohten flankierendem Massnahmen konzentriert werden, was dem Datenschutz einen Bärendienst erweist. Es wird zudem schwieriger werden, Fachleute für die betreffenden Stellen in den Unternehmen zu gewinnen, da sie sich einem Strafbarkeitsrisiko aussetzen. Eine Versicherung ist nicht erlaubt. Profitieren werden vor allem die externen Rechtsberater, was die Kosten massiv nach oben treiben wird. Die Regelung ist auch von behördlicher Seite ineffizient, da künftig zwei parallele Verfahren geführt werden müssen, eines vom EDÖB und eines von den kantonalen Strafverfolgungsbehörden, die zudem nicht über das erforderliche Know-how verfügen. Ferner ist bei diversen der Antragsdelikte unklar, wer überhaupt antragsberechtigt ist bzw. von wem der Strafantrag ausgehen sollte (z.B. bei einer unterlassenen Datenschutzfolgeabschätzung). Zudem stellt sich insbesondere bei Pflichten, die auf Ermessensentscheidungen beruhen, die Frage, inwieweit sich diese überhaupt dazu eignen, bestraft zu werden. Als Beispiele können hier die Verstösse

					gegen Art. 11 (Sicherheit von Personendaten), Art. 16 (Datenschutz-Folgeabschätzung), Art. 18 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen) sowie Art. 19 Abs. 1 (Dokumentation der Datenbearbeitungen) genannt werden. So muss beispielsweise die Dokumentationspflicht nach Art. 19 Abs. 1 VE-DSG so erfüllt werden, «dass den Informations- und Meldepflichten nachgekommen werden kann» und eine Datenschutz-Folgenabschätzung nach Art. 16 VE-DSG muss durchgeführt werden, «wenn die Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die betroffene Person führt». Das strafrechtliche Bestimmtheitsgebot erscheint jedenfalls nicht eingehalten. Die Bestrafung fahrlässigen Verhaltens ist nicht sachgerecht und auch europarechtlich nicht erforderlich. Dieses wird die vorstehend beschriebenen unerwünschten Folgen verstärken. Die Begehung des Tatbestandes durch fahrlässiges Verhalten ist daher komplett zu streichen. Eine Sanktionierung sollte nach Ansicht des VUD primär das Unternehmen betreffen. Die diesbezügliche Regelung im Vorentwurf nützt nichts, da die Mitarbeiter sich nicht darauf verlassen können, dass sie zur Anwendung gelangt. Auch ist die Grenze mit CHF 100'000 zu tief. Sie sollte bei CHF 250'000 bis 500'000 liegen. Warum die Verfolgungsverjährung auf fünf Jahre ausgedehnt wird, ist ebenfalls nicht nachvollziehbar. Für die Verschärfung der heute in Art. 35 DSG geregelten beruflichen Schweigepflicht besteht kein Anlass. Die Norm ist so zu belassen, wie sie ist. Die vorgeschlagene Anpassung würde zahlreiche Unternehmen zur Befolgung eines scharfen Berufsgeheimnisses zwingen, für das kein Bedarf besteht und das in der Praxis auch nicht gelebt würde. So ist nicht einzusehen, warum ein Online-Shop den faktisch selben Geheimhaltungspflichten wie ein Arzt oder Anwalt unterliegen soll.
RIN	StGB	179novies			Der Begriff „unbefugte Datenbeschaffung“ muss klar definiert werden. Dieser Ausdruck ist bereits bis anhin nicht klar geregelt in der Strafliteratur und es Bedarf der Rechtssicherheit. Dies auch gerade im Hinblick darauf, dass der Artikel nun auch auf Personendaten Anwendung findet und nicht wie bis anhin „nur“ auf besonders schützenswerte Daten und Persönlichkeitsprofile beschränkt ist. Dadurch, dass nun auch das unbefugte Beschaffen von Personendaten auf Antrag pönalisiert wird, eröffnet sich ein weitaus weiterer Anwendungsbereich für diesen Artikel. So kann durchaus nun auch ein Journalist nun von dieser Norm erfasst sein.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten