## Amstutz Jonas BJ

**Von:** temporaryimad@gmail.com im Auftrag von imad aad <imad@aad.name>
**Gesendet:** Dienstag, 4. April 2017 23:11
**An:** Amstutz Jonas BJ
**Betreff:** Suggestion pour l'avant projet de la LPD
**Anlagen:** Revision-totale-de-la-loi-sur-la-protection-des-donnees_Formulaire-pour-prise-de-position_fr.doc

Bonjour Monsieur,

Veuillez trouver SVP en pièce jointe une suggestion pour l'avant projet de la LPD. J'espère qu'elle soit pertinente, sachant que je ne suis pas juriste mais plutôt du côté technique de la protection de la sphère privée.

Je reste à votre disposition pour toute autre information ou clarification.

Meilleures salutations,

Dr. Imad Aad

**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 : Imad Aad

Abréviation de la société / de l'organisation :

Adresse : [redacted]

Personne de référence :

Téléphone : [redacted]

Courriel : [redacted]


Date : 4.4.2017

**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 : |
|---|---|
| Imad Aad | Remarque:<br><br>Un des principes de la LPD est l'exactitude des données traitées sur la personne concernée. Ceci est d'une grande importance dans la plupart des contextes "traditionnels" tels que les banques, les assurances maladie etc.<br><br>Cependant, certaines techniques de préservation de la sphère privée (tel que la differential privacy, entre autres) sont basées sur l'introduction d'inexactitudes dans les données: lors de la récolte de données (ex. age), une "erreur" est introduite dans chaque donnée individuelle (ex. ajouter aléatoirement un nombre entre -10 et 10). En regardant la population entière, les erreurs se compensent, et le résultat statistique (ex. moyenne d'age) est bien valide. Par contre, les données individuelles sont erronnées, en faveur de la préservation de la vie privée des individus.<br><br>On peut faire la même observation sur la technique de "déni plausible": En récoltant les données auprès des personnes concernées (ex. pour une certaine maladie), on leur permet de "mentir" avec une certaine probabilité (ex. 10%). Le résultat statistique sur la population entière reste valide avec une marge d'erreur (ex.10%), par contre chaque individu pourra ultérieurement nier l'information, en faveur de sa vie privée.<br><br>La même remarque porte sur d'autres techniques qui suivent le même principe.<br><br>Suggestion:<br><br>Ces techniques, de plus en plus utilisées de nos jours, risquent d'être illicites si la nouvelle loi n'en tient pas compte. Une dérogation pour certains contextes, par exemple avec le consentement le la personne concernée, pourra résoudre le problème favorisant l'utilisation de ces techniques et leurs effets positifs sur la protection des données. |
| | |
| | |
| | |

**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**

## 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 : |
|---|---|---|---|---|---|
| Imad Aad | LPD | 4 | 5 | | Introduire une dérogation pour les cas cités dans les remarques générales |
| Imad Aad | LPD | 50 | 1 | a | Introduire une dérogation pour les cas cités dans les remarques générales |
| | | | | | |
| | | | | | |
| | | | | | |

## 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 : |
|---|---|
| | |
| | |
| | |

## Rapport explicatif (excepté chap. 8 « Commentaire des dispositions»)

| nom/société | chap. n° | 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 : chap. 8 « Commentaire des dispositions »** | | |
|---|---|---|
| **nom/société** | **art.** | **remarque / suggestion :** |
| | | |
| | | |
| | | |

## Amstutz Jonas BJ

**Von:** Fritz Abbühl <fritz.abbuehl@sicherheitsteam.ch>
**Gesendet:** Sonntag, 2. April 2017 20:10
**An:** Amstutz Jonas BJ
**Betreff:** Stellungnahme zur Vernehmlassung
**Anlagen:** VernehmlassungDSG.doc

Sehr geehrter Herr Amstutz

In meiner beruflichen Tätigkeit sehe ich immer wieder, dass dem Schutz von Personendaten nicht das angemessene Gewicht gegeben wird. Die Auswirkungen können für die direkt betroffenen Personen, die Firmen und endlich auch für die Schweiz fatal sein.
Von Kollegen aus Deutschland weiss ich, dass dort die Sache sehr viel ernster als in der Schweiz genommen wird. Bereits die heutige gesetzlichen Grundlagen, insbesondere auch deren Durchsetzung, erachte ich im Vergleich als „Schwachstrom“. Eine weitere Schwächung, auch in Hinblick auf die zunehmenden Gefährdungen wäre ein tragischer Fehlentscheid.
Wir brauchen eine viel stärkeren Datenschutz! Daher nehme ich ausdrücklich gegen jegliche Schwächung Stellung!
Ich bitte Sie meine Stellungnahme entsprechend weiterzuleiten.

Besten Dank.

Freundliche Grüsse

Fritz Abbühl

---

Sicherheitsteam.ch

Fritz Abbühl
Security- und EHS-Manager CFPA / SAQ / EKAS | BDSV nach DSG CH | IT-Services Engineer HF
Rütschistrasse 16, 8037 Zürich | M:*+41 76 824 01 44* | P: +41 44 361 45 02 | fritz.abbuehl@sicherheitsteam.ch
www.sicherheitsteam.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 : Sicherheitsteam Fritz Abbühl

Abkürzung der Firma / Organisation :

Adresse : Rütschistrasse 16

Kontaktperson : Fritz Abbühl, Eigentümer

Telefon : +41 76 824 01 44

E-Mail : fritz.abbuehl@sicherheitsteam.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

**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 |
|---|---|
| | **Verzicht auf den bDSB schwächt den Datenschutz**<br><br>**1 Einleitung**<br><br>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».<br><br>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.<br><br>**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**<br><br>**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).<br><br>**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.**<br><br>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.<br><br>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).**<br><br>**2 Historische Entwicklung**<br><br>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.<br><br>Basierend auf der revidierten Fassung des DSG haben bis 27. Januar 2017 über 1000 Unternehmen ihren Betrieblichen Datenschutzverantwortlichen dem EDÖB formell gemeldet. |

| | |
|---|---|
| | **3 Internationaler Vergleich**<br><br>**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).<br><br>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*).<br><br>**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**.<br><br>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.<br><br>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 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**<br><br>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).<br><br>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.<br><br>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).<br><br>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.<br><br>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 Einsatz eines Datenschutzbeauftragten mit entsprechenden Erleichterungen bzw. Ausnahmen seitens Bundesrat/Verordnung ist hingegen zu empfehlen.<br><br>**5 Notwendigkeit eines DSB in der Praxis**<br><br>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.<br><br>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.<br><br>**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.**<br><br>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.**<br><br>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.<br><br>**6 Fehlende Begründung**<br><br>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.<br><br>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.<br><br>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.<br><br>**7 Anträge**<br><br>Aufgrund dieser Überlegungen wird der Antrag gestellt, die Funktion des «Betrieblichen Datenschutzbeauftragten» im Datenschutzgesetz wie folgt zu berücksichtigen:<br><br>**Neuer Artikel 11$^{bis}$: Bezeichnung eines Betrieblichen Datenschutzbeauftragten**<br><br>1 Verantwortliche und Auftragsbearbeiter können einen Datenschutzbeauftragten bezeichnen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht.<br><br>2 Zur Bezeichnung eines Datenschutzbeauftragten sind verpflichtet<br><br>a. Bundesorgane wenn sie Personendaten bearbeiten<br><br>b. Auftragsbearbeiter wenn sie als wesentlicher Teil ihrer geschäftlichen Verrichtungen Personendaten für Verantwortliche bearbeiten<br><br>c. Verantwortliche<br><br>wenn sie zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet sind, oder<br><br>wenn sie mehr als zehn Personen ständig mit der Bearbeitung personenbezogener Daten selbst oder über Dritte beschäftigen, oder<br><br>wenn sie ohne gesetzliche Pflicht als wesentlicher Teil ihrer geschäftlichen Verrichtungen regelmässig<br><br>1 besonders schützenswerte Personendaten Dritter bearbeiten oder personenbezogenes Profiling betreiben; |

| | |
|---|---|
| | 2 Personendaten nicht bei der betroffenen Person beschaffen;<br>3 Personendaten an Dritte bekanntgeben;<br>4 Personendaten ins Ausland bekanntgeben;<br>5 Entscheidungen über Personen treffen, die ausschliesslich auf einer automatisierten Datenbearbeitung beruhen.<br>3 Der Datenschutzbeauftragte kann Arbeitnehmer des Verantwortlichen oder des Auftragsbearbeiters sein oder seine Aufgaben im Auftragsverhältnis erfüllen.<br>4 Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und dem Beauftragten mitzuteilen.<br>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.<br><br>**Ergänzung in Art. 6 Abs. 2 Bekanntgabe ins Ausland in Ausnahmefällen (roter Text):**<br>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.<br><br>**Neuformulierung Art. 16 Abs. 3 Datenschutz-Folgeabschätzung (roter Text):**<br>[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.<br><br>**Neuer Art. 17 Abs. 5 Meldung von Verletzungen des Datenschutzes (roter Text):**<br>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. |

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

| Name/Firma | Gesetz | Art. | Abs. | Bst. | Bemerkung/Anregung |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

## 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:** Daniel Kettiger <daniel.kettiger@vtxmail.ch>
**Gesendet:** Donnerstag, 9. März 2017 11:08
**An:** Amstutz Jonas BJ
**Cc:** Dubois Camille BJ
**Betreff:** Vernehmlassung Datenschutzgesetz; Bemerkungen zu Art. 10 VE-DSG (Zertifizierung)

Sehr geehrte Damen und Herren

Im heutigen Art. 11 Abs. 1 DSG ist die Zertifizierung wie folgt umschrieben bzw. geregelt:
Um den Datenschutz und die Datensicherheit zu verbessern, können die Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Bundesorgane, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

Neu soll Art. 10 Abs. 1 VE-DSG die Zertifizierung grundlegend wie folgt regeln:
Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen.
Les responsables du traitement et les sous-traitants peuvent soumettre leurs opérations de traitement à une évaluation effectuée par des organismes de certification agréés et indépendants.

Laut dem Kommentar im Erläuternden Bericht soll die neue Formulierung im VE-DSG weiter gefasst sein und den Gegenstand der Zertifizierung ausdehnen. Neu sollen neben Verfahren und Organisation sowie Produkten (Programmen, Systemen) auch Dienstleistungen zertifiziert werden können.

Genau das ist aber gemäss dem neuen Gesetzestext nicht der Fall – der neue Gesetzestext ist einschränkender als der heutige und fokussiert nur auf Datenbearbeitungsvorgänge. Der Begriff „Vorgang" bezeichnet in der hier massgeblichen betriebswirtschaftlichen Terminologie einen Prozess. Mit dem Begriff „Datenverarbeitungsvorgänge" sind somit nur die Prozesse der Datenbearbeitung Gegenstand der Zertifizierung, nicht jedoch – wie offenbar gewollt – auch Produkte oder Dienstleistungen (z.B. Cloud-Dienstleistungen). Der französische Begriff von „opération de traitement" ist ähnlich eng und fokussiert auch auf betriebliche Abläufe. Die Anlehnung an den Wortklaut der deutschen Übersetzung von Art. 42 der Verordnung (EU) 2016/679 ist unbehelflich, weil dieser Text genauso einengend und auf Prozesse fokussierend ist.

Weiter können neu nur noch die Verantwortlichen und Auftragsdatenbearbeiter eine Zertifizierung beantragen bzw. durchführen lassen. Bei Produkten ist dies nicht sinnvoll. Bei Produkten ist es sinnvoll, dass – wie heute im DSG vorgesehen – die Hersteller die Produkte zertifizieren lassen können. Ansonsten muss das gleiche Produkt bei jedem Nutzer als Verantwortlicher für Personendaten erneut zertifiziert werden.

M.E. ist Art. 11 VE-DSG total missraten und bedarf einer Neuformulierung von Grund auf.

Freundliche Grüsse
Daniel Kettiger

---

**Daniel Kettiger**
Rechtsanwalt/Mag.rer.publ.
kettiger.ch - law§solutions
Birkenweg 61
CH-3013 Bern
Fon +41 31 335 68 67
Mail info@kettiger.ch
Web http://www.kettiger.ch

**Beat Lehmann**
lic.iur. Fürsprech
Acting Counsel Alcan Holdings Switzerland
Postfach 3244
5001 Aarau
Tel 079 – 500 82 32
b.lehmann-aarau@bluewin.ch

Aarau, 4. April 2017

# Stellungnahme

## zum Entwurf für eine Totalrevision des Datenschutzgesetzes ("Rev-E DSG")

## A. Allgemeines

Die nachstehenden Überlegungen sind aus der Mitwirkung des Unterzeichnenden an der Vernehmlassung zur sog "Totalrevision des DSG" in verschiedenen Wirtschafts- und Informatik-Organisationen sowie aus der kritischen Auseinandersetzung mit dem von der Vereinigung der im öffentlichen Bereich tätigen Datenschutzbeauftragten "privatim" über veröffentlichten Stellungnahme für ein "Zeitgemässes Datenschutzgesetz für die Schweiz" entstanden. https://www.privatim.ch/files/layout/downloads_de/privatim_Stellungnahme_VE-DSG.pdf Sie befassen sich mit ausgewählten Aspekten der Weiterentwicklung des Datenschutzes im privaten Bereich.

Die aktuelle Entwicklung, insbesondere das durch die Datenschutzgrundverordnung ("DSG-VO") harmonisierte Recht zeigt, dass das Datenschutzrecht als sog "Querschnittsmaterie" zu einem der komplexesten Rechtsetzungsprojekt überhaupt geworden ist. Denn der Datenschutz bezieht sich auf den umfassenden Umgang mit den allgegenwärtigen personenbezogenen Angaben in der modernen Informationsgesellschaft.

Nach hier vertretener Auffassung haben vor allem folgende Umstände zum Auftrag des Bundesrates beigetragen eine Totalrevision des DSG an die Hand zu nehmen:

### A.1 Einflüsse aus der Entwicklung im Europäischen Umfeld

A.1.1 Diesbezüglich ist zunächst auf den Erlass der **europäischen Datenschutz-Grundverordnung** ("DSGVO") vom 4. Mai 2016 hinzuweisen welche ab 25. Mai 2018 in allen EU Ländern Geltung haben wird und aufgrund von Art. 3 auch auf jene Schweizer Unternehmen anwendbar ist, vor allem wenn sie im Europäischen Wirtschaftsraum ("EWR") ihre Produkte und Dienstleistungen anbieten.

A.1.2 Die Aufrechterhaltung des freien Datenverkehrs (*"free flow of information")* mit Kunden und Geschäftspartnern im EWR ist für Schweizer Unternehmen unabdingbar. Daher drängt sich unter diesem Titel eine gewisse Anpassung des künftigen schweizerischen Datenschutzgesetzes ("CH-DSG") an die DSGVO auf, um die Voraussetzungen für einen "**Angemessen-**

**heitsbeschluss**“ der Kommission nach Art. 45 DSGVO betreffend Gleichwertigkeit des schweizerischen Schutzniveaus mit dem Stand des Datenschutzes im EWR zu schaffen.

A.1.3 Allerdings unterscheiden sich die Anforderungen aus Art. 45 DSGVO nicht grundlegend von den entsprechenden Regeln von Art. 25 der bisher geltenden Richtlinie 95/46/EG und der Arbeitsunterlage der Arbeitsgruppe 29 vom 24. Juli 1998 betreffend die Übermittlung personenbezogener Daten in Drittländer gemäss Art. 25 und 26 der Datenschutzrichtlinie 95/46/EG http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf

A.1.4 Auf dieser Grundlage hat die Kommission mit Entscheidung vom 26. Juli 2000 die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz nach dem damals in Bund und Kantonen geltenden Rechtszustand verbindlich festgestellt http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32000D0518&from=EN Man könnte daher in guten Treuen davon ausgehen und behaupten, dass sich durch den Erlass der DSGVO an diesem Zustand nichts ändern sollte, umso mehr als nach Art. 45 (9) DSGVO die unter dem Regime von Art. 25 (6) der Richtlinie 95/46/EG getroffenen Feststellungen der Kommission über die Gleichwertigkeit des schweizerischen Datenschutzes bis zur bevorstehenden nächsten periodischen Überprüfung aufrecht bleiben.

A.1.5 Darüber hinaus verlangt auch in Zukunft der Feststellungsbeschluss der Kommission von einem Drittland ausserhalb der EU **keine unveränderte, wörtliche oder inhaltliche Übernahme der Datenschutzvorschriften der DSGVO** [welche übrigens ja erhebliche Freiräume für die nationale Umsetzung erlaubt, wie dies durch den umfangreichen und in der Datenschutz-Szene kontrovers diskutierten Gesetzentwurf der Bundesregierung für ein ”Datenschutz-Anpassungs- und Umsetzungsgesetz – EU” (” DSAnpUG-EU”) dokumentiert wird]. Vielmehr wird auch in Zukunft die Angemessenheit des in der Schweiz gebotenen Schutzniveaus gemäss Art. 45 (2) DSGVO nach einen umfangreichen Komplex von Beurteilungskriterien geprüft werden wie namentlich die Rechtsstaatlichkeit, die Achtung der Menschenwürde und Grundfreiheiten, das Vorhandensein von Rechtsvorschriften zum Datenschutz, Berufsregeln und Vorschriften zur Datensicherheit, die Praxis der Gerichte, wirksame Rechtsbehelfe zur Durchsetzung der Ansprüche betroffener Personen, die Existenz unabhängiger Behörden, die mit der Einhaltung und Durchsetzung des Datenschutzes betraut sind, sowie die vom betreffenden Drittland eingegangenen internationalen Verpflichtungen (wie z.B. der vorgesehene Beitritt unseres Landes zu dem in Modernisierung begriffenen Datenschutzübereinkommen SEV 108 des Europarates https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/entw-konvention-d.pdf , oder das im Nachgang zu dem entsprechenden Abkommen der EU mit der U.S.A. vereinbarte und vom Bundesrat am 11.01.2017 genehmigte ”Swiss US Privacy Shield“ für den datenschutzkonformen Informationsverkehr mit den Vereinigten Staaten. https://www.edoeb.admin.ch/datenschutz/00626/00753/01405/01406/index.html?lang=de

A.1.6 Angesichts der vorstehenden Überlegungen erscheint die in gewissen Kreisen der Wirtschaft verbreitete Besorgnis, die Schweiz könne ihren Status als Drittland mit angemesse-

nem Datenschutzniveau verlieren, als einigermassen übertrieben. Dabei ist allerdings darauf hinzuweisen, dass die EU Kommission aufgrund der nicht restlos gelösten Probleme um die Personenfreizügigkeit die Überprüfung nach Art. 45 DSGVO zum Anlass nehmen könnte, Druck auf die Schweiz und deren Wirtschaft auszuüben, und dass es gegen eine künftige negative Beurteilung des schweizerischen Schutzniveaus im Datenschutz kein uns bekanntes Rechtsmittel gibt. Es rechtfertigt sich daher nach dem "**Vorsichtsprinzip**", eine etwas weitergehende Harmonisierung des DSG mit dem europäischen Datenschutzrecht anzustreben, wobei die Schweiz als souveränes Drittland mit einem heute schon international anerkannte hohen Stand des Datenschutzes zweifellos nicht verpflichtet ist, die ausufernden und teilweise lebensfremden Bestimmungen der DSGVO (Beispiel: Datenschutz bei Kindern nach Art. 8 DSGVO) unverändert zu übernehmen.

A.1.7 Die Harmonisierung des künftigen CH-DSG mit dem europäischen Datenschutzrecht ist nach hier vertretener Auffassung für Schweizer Unternehmen namentlich unter folgenden Gesichtspunkten relevant:

(i) Kunden, Lieferanten, Geschäftspartner und Auftragsbearbeiter von Schweizer Unternehmen im EWR dürfen personenbezogene Daten frei an Empfänger in der Schweiz übermitteln. Mit anderen Worten: Die Angemessenheit des CH-DSG ist vor allem für den **Export von Personendaten aus dem EWR** an Empfänger in der Schweiz relevant.

(ii) Bei der Harmonisierung des künftigen CH-DSG mit den Anforderungen aus der DSGVO sollte angestrebt werden, dass Schweizer Firmen, welche im EWR tätig sind und Art. 3 der DSGOV dem harmonisierten europäischen Datenschutzrecht unterstehen sich datenschutzrechtlich an die Anforderungen der DSGVO halten könne weil sie davon ausgehen dürfen, dass sie damit auch die Plichten aus dem CH-DSG erfüllen. Mit anderen Worten (i) das künftige CH-DSG sollte n i c h t Vorschriften und Plichten aufstellen, welche als sog. "*Swiss Finish*" über die Anforderungen des harmonisierten europäischen Datenschutzrecht hinausgehen**;** und (ii) darüber hinaus sollten sich die im EWR tätigen Schweizer Unternehmen darauf verlassen dürfen, dass sie bei Beachtung der Vorschriften der DSGVO auch die Anforderungen des künftigen CH-DSG einhalten.

### A.2 Berücksichtigung der Technologische Entwicklung

A.2.1 Das geltende DSG von 1992/2006 beruht auf dem Stand der Datenbearbeitung in den 80er und 90er Jahren, also weit vor dem Eindringen der Informatik in sämtliche Lebensbereiche und der damit verbundenen unübersehbaren - und oft grenzüberschreitenden!- automatisierten Erfassung und Bearbeitung personenbezogener Daten, wie beispielsweise die Integration von Datenverarbeitung und Telekommunikation, der Siegeszug des Internet, die Verlockungen der sozialen Netzwerke, die Verlagerung ("*Outsourcing*") der Datenverarbeitung in der "*Cloud*", das Eindringen der Informatik in die gesamte Kette industrieller Produktion und Wertschöpfung ("Industrie 4.0" und die Ausbreitung intelligenter Gegenstände ("*Internet of Things*", auch in Form "*wearable devices*") Steuerung der Stromnetzte durch "*smart grid*", die Digitalisierung der Medizin durch "*e-healt"h*, die Vermischung der berufli-

chen und privaten Sphäre ("*Bring Your Own Device*" - BYOd), die Auswertung vorhander Datenbestände durch "*Big Data Analytics*", das Auftrete neuer Arten der Bedrohung der Datensicherheit (APT – "*Advanced Persistent Threat*", *DDoS*, "*Ransomware*"), das Aufkommen erster autonom gesteuerter Fahrzeuge.

A.2.2 Eine klare Antwort auf diese neuen technologischen Herausforderungen ist allerdings entgegen der Darstellung der Vereinigung "privatim" weder in der DSGVO noch im RevE DSG zu finden. Das spricht einerseits für die Bedeutung der von den Schöpfern des DSG 1992 angestrebten **technischen Neutralität** des Gesetzes, bedeutet andererseits aber die nüchterne Einsicht, dass es dem Gesetzgeber weder im EWR noch in der Schweiz gelungen ist, für die technologischen Herausforderungen der "*Brave New Data World*" in Wirtschaft, Verwaltung und Gesellschaft eine schlüssige Umsetzung in praktisch durchführbare Datenschutzvorschriften zu entwickeln.

A.2.3 Es wäre nach hier vertretener Auffassung aber auch nicht zielführend, im DSG und dessen Ausführungsgesetzgebung für jede sich abzeichnende neue Form der Bearbeitung von Personendaten eine verbindliche Regelung aufzunehmen: **Das Datenschutzrecht muss technologisch offen bleiben.** Neue Herausforderungen werden am besten durch "**Verhaltensregeln**" im Sinne von bzw. "**Empfehlungen** Art. 40/41 DSGVO **der guten** Praxis" nach Art. 8 RevE DSG flexibel gemeistert, welche vom Beauftragten in Zusammenarbeiten mit Berufsverbänden wie VUD, swico oder ISSS, bzw. Finma/Bankiervereinigung, oder von Berufsverbänden mit Genehmigung des Beauftragten, z.B. Swiss Marketing, Schweiz. Versicherungsverband ASV/SVV aufgestellt werden (vgl. den weit verbreiteten Datenschutzkodex der deutschen Versicherer http://www.gdv.de/2013/09/versicherungsunternehmen-treten-datenschutzkodex-bei/ ) **Die bewährten Grundsätze des Datenschutzes sollten somit weiterhin ungeachtet künftiger Weiterentwicklungen der Informatik anwendbar bleiben.**

### A.3 Die Anwendung des Datenschutzrechts im Privatbereich - ein "Mengenproblem"

A.3.1 Bei jeder Änderung von Anforderungen an den Datenschutzes für die bearbeitenden Stellen im privaten Bereich sollte unbedingt die **Tragweite der Auswirkungen** beachtet werden: Es gibt in unserem Lande **rund 750'000 Organisationen** welche in ihrer Mehrheit auch Personendaten bearbeiten: Rund **550'000 Unternehmen**, darunter befinden sich mehr als 95% KMU mit weniger als 100 Beschäftigten https://www.kmu.admin.ch/kmu/de/home/kmu-politik/kmu-politik-zahlen-und-fakten/kmu-in-zahlen/firmen-und-beschaeftigte.html; es gibt im Weiteren ungefähr **100'000 Vereine** https://www.nzz.ch/die-vereine--die-heimlichen-paedagogen-1.8968129 ; über **13'000 Stiftungen** http://www.swissfoundations.ch/sites/default/files/STIFTUNGREPORT2016_DE_v16c_1.pdf und gemäss dem Bericht des Bundesrates über die freien Berufe in der Schweiz vom 15. 1.2014 **mehr als 70'000 freiberuflich tätige Personen** wie Ärzte, Anwälte, Notare, Revisoren, Architekten und Ingenieure, Unternehmens- und Steuerberater, ICT Consultants und ICT Sicherheitsberater).

A.3.2 Auch wenn nicht alle diese ca. 750'00 Organisationen - und nicht nur die in Datenschutz-Kreisen gerne erwähnten "**global tätigen Grossunternehmen**" - in relevantem Umfang Daten über Per-

sonen bearbeiten und ins Ausland bekanntgeben, entsteht ein erhebliches **Mengenproblem**. Denn die datenbearbeitenden Stellen haben ohne Ausnahmen bei ihrer zunehmend automatisierten Bearbeitung von Personendaten sämtliche Regeln des Datenschutzes strikt einzuhalten. Dabei muss davo ausgegangen werden, dass heute und erst recht in der Zukunft heikle Beschaffungen, Bearbeitungen und Auswertungen personenbezogener Daten gerade **auch durch kleine und kleinste Unternehmen** (sog. "*ICT Startups")* vorgenommen werden (vgl. deren Tätigkeitsbereiche auf der Webseite http://www.startup.ch/index.cfm?page=129574 )

A.3.3 In der Arbeitsgruppe des Bundes zur Schaffung des DSG-92 wurde die - rückblickend etwas blauäugig erscheinende - These vertreten, dass ein Bearbeiter von Personendaten die Pflichten aus dem Datenschutz ohne weiteres einhält, wenn er - in Küchenlatein ausgedrückt - als "*bonus gestor datorum*" mit personenbezogenen Angaben über seine Kunden, Geschäftspartner, Angestellten und Benutzer treu, sorgfältig und rücksichtsvoll umgeht. Von diesem ursprünglichen "romantischen Datenschutzgrundsatz" hat sich die Rechtsentwicklung inzwischen sehr weit entfernt.

A.3.4 Es gibt übrigens noch einen weiteren in Gesetzgebung und Literatur wenig behandelten Aspekt der Mengenproblematik: Die bei den datenbearbeitenden Stellen von Wirtschaft und Verwaltung in sehr grossem Umfang vorhandenen **Archiv-** und (oft in mehreren" Generationen" vorhandenen) **Sicherungs-Dateien**. So ist gemäss § 19 (2) sowie § 34(7) iVm § 33 (2) Ziff. 2 BDSG **keine Auskunft über Daten** zu erteilen, welche lediglich für Archiv- oder Sicherungszwecke gespeichert sind und die Auskunftserteilung einen übermässig hohen Aufwand bedeuten würde. Aber auch andere Pflichten aus dem RevE DSG (z.B. Art. 19 b RevE DSG: Pflicht zur Information über die Löschung von Daten (auch in einer Sicherungsdatei?) sind darauf zu überprüfen, ob sie auch für Archiv- und Sicherungsdaten anwendbar sind.

A.3.5 Daraus ergibt sich nach hier vertretener Auffassung, dass die Anforderungen aus dem Datenschutz einfach, klar und ohne weiteres umsetzbar sein müssen und dass von einem **komplexen Regelwerk mit weitreichenden administrativen und erst noch strafbewehrten Prüf-. Konsultations-, Melde-, Informations- und Anzeigepflichten unbedingt abzusehen** ist.

A.3.6 Aus der vorstehend umschriebenen **Mengenproblematik** folgt aber auch, dass jede neue Pflicht aus dem Datenschutz (wie z.B. die Meldepflicht bei Auslandbekanntgaben nach Art. 5 Abs. 3 Bst b) RevE DSG in der heutigen globalisierten Arbeits- und Freizeit-Welt; die Einführung einer Rechtspflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten; die erweiterten Informationspflichten unter Art. 13 RevE; die Informations- und Anhörungspflicht bei automatisierten Einzelentscheidungen nach Art. 15 RevE DSG (auch beim Abheben von Geld aus einem Geldautomaten nach automatischer Kontenüberprüfung?); die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 16 RevE DSG), oder die Pflicht zur Meldung von Datenschutzverletzungen nach Art. 17 RevE DSG) unter dem Gesichtspunkt der praktischen Auswirkungen zu würdigen ist, wenn diese Pflichten durch tausende und abertausende von bearbeitenden Stellen rechtskonform umgesetzt werden sollen.

A.3.7 Das "Mengenproblem bei der Datenschutzgesetzgebung im privaten Bereich" kann nach hier vertretener Auffassung namentlich durch folgende Regelungen einigermassen beherrscht werden:

(i) die entsprechenden Bestimmungen sind - auch im Vergleich zu den entsprechenden Regelungen der DSGVO – nach Möglichkeit **auf die für den Datenschutz wirklich kritischen Vorgänge** zu beschränken; und

(ii) es kann sich im Einzelfall empfehlen, bei den unter vorstehender Ziff. A.3.6 umschriebenen Regelungen dem Bundesrat die Kompetenz einzuräumen, gewisse alltägliche Vorgänge von der Vorschrift auszunehmen (vgl. die Ausnahmen von der Anmeldungspflicht gemäss Art. 4 und 18VDSG).

## A.4 Hinweis auf Datenschutzprobleme im Bereich der öffentlichen Verwaltung

A.4.1 Es darf im Zusammenhang mit der Revision der Datenschutzgesetzgebung aus der Sicht eines Juristen, welcher damit vertraut ist, dass die Informationstätigkeit seiner Gesellschaft, wie auch ihrer Geschäftspartner, sich auf den rationellen und marktkonformen Vertrieb von Gütern und Dienstleistungen ausrichtet, nicht unterwähnt bleiben, dass im **Bereich der (Bundes-)Verwaltung und halbstaatlicher Unternehmen** unter Schlagworten wie *"EGoverment*", "*Digitale Schweiz*", "*Strategische Informationsgesellschaft*" und "*Digitale Transformation*" verschiedene Initiativen, Konzepte und Projekte angedacht, geplant, angebahnt oder bereits realisiert sind, welche die **Privatsphäre und ds Recht auf informationelle Selbstbestimmung der Bürger erheblich beeinträchtigen** (vgl. den Leitentscheid BGE 124 I 176 Erw. 6.a mit Hinweisen) und auch zu **schwerwiegenden Problemen der Informatiksicherheit** führen können, o h n e dass mit den betreffenden Anwendungen aus unternehmerischer Sicht ein eindeutig ausgewiesener praktischer Nutzen verbunden ist.

A.4.2 Dazu gehören nach hier vertretener, auf langjährige Erfahrungen mit Informatikanwendungen in Wirtschaft und Verwaltung zurück gehender Auffassung verschiedene Projekte, die entgegen dem Auftrag der Bundesverfassung (Art. 43a Abs. 5 BV) den Praxistest der Wirtschaftlichkeit kaum bestehen würden. Denn **nicht alles, was durch den Einsatz der Informatik machbar ist, macht auch Sinn**. Ohne Anspruch auf Vollständigkeit seien folgende Projekte erwähnt:

a. Die entgegen dem (nun bezeichnenderweise aufgehobenen!) Vorbehalt von Art. 36 Abs. 4 Bst. c DSG-92 von der Verwaltung angestrebte Nutzung der **Sozialversicherungsnummer als universelles Identifikationsmittel** https://www.nzz.ch/newzzEAS0SAVC-12-1.155273 was die Zusammenführung der von der Verwaltung erhobenen Personendaten und das Erstellen eigentlicher Persönlichkeitsprofile erheblich erleichtern kann.

b. Das von der Bundeskanzlei gehätschelte, in der Anwendung aufwändige und komplizierte **Prestigeprojekt "E Voting"** als kostspielige Ergänzung der bewährten Verfahren zur persönlichen oder brieflichen Stimmabgabe https://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de

c. Das "**elektronische Patientendossier**" dessen Pilotanwendungen bereits schwere Mängel offenbart haben http://www.computerworld.ch/news/it-branche/artikel/walliser-patientendossier-bereits-wieder-offline-68625/ das für die Medizin nach einhelliger Auffassung der Spitäler und Ärzteorganisationen kaum greifbare Vorteile bietet, jedoch eine über das Internet zugängliche Datenbank mit Pa-

tientendaten schaffen soll und das wie in Grossbritannien zum **Milliardengrab** werden könnte. https://www.theguardian.com/society/2013/sep/18/nhs-records-system-10bn

d. Der Aufbau **intelligenter Stromnetze** *("smart grid")* als Teil der "Energiestrategie 2050" http://www.bfe.admin.ch/smartgrids/ mit angedachter Einbeziehung der Erfassung von Daten über die Nutzung der Hauselektronik und das Nutzungsverhalten der Stromkonsumenten; die dadurch geschaffenen zahlreichen Möglichkeiten für das Einschleusen von Schadprogramme schaffen Risiken für einen weiträumigen "***Blackout***". In diesem Zusammenhang wäre zu prüfen, ob der Datenschutz, weil das Verhalten der Angehörigen von Haushalten erfasst wird, nach dem Vorbild von § 4 Ziff. 3 des österreichischen Datenschutzgesetzes 20000 in Zukunft nicht auch "bestimmbare Personengemeinschaften" umfassen sollte.

e. Die vom Eidgenössischen Datenschutzbeauftragten beanstandete Erfassung und Auswertung der "**Swiss Pass" Kontrolldaten** durch die Anbieter des öffentlichen Verkehrs www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-60675.html

f. Das Projekt "**Elektronische Vignette**": Ein ökonomisch zweifelhafter Ersatz des heute geübten Aufklebens der Vignette durch deren elektronische Registrierung und Datenerfassung https://www.ezv.admin.ch/ezv/de/home/aktuell/medieninformationen/medienmitteilungen.msg-id-64772.html

g. **"Mobility Pricing"** mit Erfassung der Mobilitätsdaten der Benützer von öffentlichen Verkehrsmitteln. https://www.astra.admin.ch/astra/de/home/themen/mobility-pricing.html

h. **Road Pricing**" mit Erfassung der Bewegungsdaten der Verkehrsteilnehmer http://www.news.admin.ch/NSBSubscriber/message/attachments/7432.pdf

A.4.3 Zusammen mit der Digitalisierung aller Informations- und Kommunikationsvorgänge und dem sorglos-unbedachten Umgang der "*digital natives*" mit den Verlockungen von Anwendungen ("*Apps*") in den sozialen Netzwerken bringen uns die vorstehend umschriebenen IKT Projekte der öffentlichen Verwaltung, welche auf die informationelle Erfassung wichtiger Lebensvorgänge abzielen, der **Zukunftsvision "1984"** sehr nahe, bzw. sie gehen in einer Art und Weise darüber hinaus, die sich der Autor George Orwell in den Jahren 1946-1948 gar nicht hat vorstellen können. Dabei versteht sich von selbst, dass sich die Initianten und Promotoren der betreffenden Projekte und Anwendungen nicht von Orwell'schen Überlegungen leiten lassen; sie tragen aber dazu bei, dass als "*unintendes consequences*" https://de.wikipedia.org/wiki/Unbeabsichtigte_Folgen einer umfassenden Kontrolle und Beeinflussung aller menschlichen Äusserungen und Handlungen durch das Risiko verbotener Einwirkungen privater oder staatlicher, inländischer und ausländischer Organe Vorschub geleistet wird.

A.4.4 Aufgrund eines Berichts des europäischen Datenschutz-Pioniers Frits Hondius an die damalige Expertenkommission zur Schaffung des DSG-92 über die Zerstörung des zentralen Bevölkerungsregisters als erste Aktion der niederländischen Widerstandsbewegung nach der deutschen Besetzung ist in Art. 36 Abs. 4 DSG des noch im Zeitalter des kalten Kriegs entstandenen DSG-92 die Bestimmung über die Sicherung von Datensammlungen enthalten, die im Kriegs- oder Konfliktfall zu einer Gefährdung von Leib und Leben betroffener Personen führen können (Botschaft vom

88.032 vom 23.03.1988, BBl 1983 S.487). Diese Bestimmung wird durch die Revision des DSG ersatzlos gestrichen. Sie ist durch die umfassende Digitalisierung aller Lebensvorgänge auch obsolet geworden. Es wäre jedoch nach hier vertretener Auffassung eine nicht berechtigte Aufgabe sich aktiv dafür einzusetzen, dass aufgrund der auch im öffentlichen Bereich ausufernden Erfassung von Personendaten in Ausübung staatlicher Hoheitsrechte der dadurch hervorgerufenen Bedrohung von Privatsphäre und Grundrechte unserer Bevölkerung verstärkt Rechnung getragen wird.

### A.5 Schaffung klarer Rechtsgrundlagen

A.5.1 Nach der in Datenschutzkreisen vertretenen Auffassung soll die Revision des DSG der "Schaffung klarer Rechtsgrundlagen" dienen. Davon kann bei kritischer Prüfung des nun vorliegenden Revisionsentwurfs allerdings im Ernste nicht die Rede sein.

A.5.2 Vielmehr beschränkt sich der revE DSG vor allem auf die Schaffung eine Anzahl zusätzlicher - vielfach sogar strafbewehrter - administrativer Melde- und Informationspflichten, welche - wenn von den bearbeitenden Stellen rechtskonform umgesetzt ernst genommen - die Infrastruktur des Beauftragen überschreiten werden. Deshalb wird denn auch von Datenschutzkreisen der personelle Ausbau der Datenschutz-Administration auf allen Stufen gefordert. Für die bearbeitenden Stellen aber, vor allem für die dem Rev DSG unterstellten Kleinen und Mittleren Unternehmen ("KMU") hätte dieses Rechtsetzungskonzept einen **erheblichen administrativen Mehraufwand** zur Folge, o h n e dass damit eine eindeutige Verstärkung des Persönlichkeits- und Datenschutzes der betroffenen Personen verbunden wäre.

### A.6 "Präventiver Datenschutz"

A.6.1 Die Forderung, im Privatbereich neben einer Datenschutz-Folgeabschätzung (Art. 16 RevE) noch eine **Vorabkonsultation** (zweifellos beim Beauftragten) einzuführen ist Ausdruck der in Datenschutzkreisen verfolgten Tendenz den Datenschutz durch ein ausgreifendes System von (oft erst noch strafbewehrten) Informations- und Meldepflichten zu ergänzen. Die in dieser Beziehung von der Vereinigung "privatim" aufgestellte Forderung geht in gewisser Weise über das harmonisierte europäische Datenschutzrecht hinaus (Art. 35/36 DSGVO). Mit einer derartigen "Vorabkonsultation" wäre auch eine erhebliche Verzögerung der Einführung neuer Anwendungen verbunden.

A.6.2 Eine (strafbewehrte) Rechtspflicht zu einer Vorauskonsultation des Beauftragten ist aber auch aus Gründen der heiklen Umschreibung der darunter fallenden Situationen abzulehnen. Im Übrigen wird der Beauftragte schon heute im Rahmen seiner gesetzlichen Beratungsaufgabe gemäss Art. 28 DSG von pflichtbewussten datenbearbeitenden Stellen für solche Konsultationen häufig in Anspruch genommen. Denn es besteht bei den bearbeitenden Stellen der Privatwirtschaft in der Praxis ein grosses Interesse daran, den Umgang mit personenbezogenen Angaben über ihre Kunden, Interessenten, Lieferanten, Mitarbeitenden und Geschäftspartner datenschutzkonform, "*privacy compliant*" abzuwickeln.

A.6.3 "**Präventiver Datenschutz**" wird nach hier vertretener Auffassung in der Praxis durch eine ganze Reihe **schon heute bestehender und bewährter Institutionen** gewährleistet wie z.B. in nicht abschliessender Aufzählung

a. **Beratung durch den EDÖB** auf Wunsch bearbeitender Stellen (Art. 28 DSG) - davon wird in der Praxis auch in erheblichem Umfang Gebrauch gemacht;

b. **vom EDÖB** erlassene und gemäss Art. 30 Abs. 2 DSG publizierte **Empfehlungen** im Rahmen von Abklärungen nach Art. 29 DSG;

c. die zahlreichen vom EDÖB (allerdings nach hier vertretener Auffasung bisher ohne klare Rechtsgrundlage) publizierten **Merkblätter und Leitfäden**;

d. Beratung und Empfehlungen durch die von vielen bearbeitenden Stellen eingesetzten internen oder **externen betrieblichen Datenschutzbeauftragten** (Art. 11a Abs. 5 Bst. e DSG und Art. 12a und 12b VDSG; Art. 37-38 DSGVO); die Unterlassung der Erwähnung des bDSB im RevE DSG ist nach hier vertretener Auffassung ein unverzeihlicher Verstoss gegen einen wirksamen Datenschutz in der Praxis!

e. **Zertifizierung** von Datenschutz-Management-Systemen (Art. 11 DSG und VDSZ);

f. **Standesregeln** und "*good practice*" von Berufs- und Wirtschaftsorganisationen (vgl.dazu Art. 27 RL 95/46/EG; Art. 40 DSGVO; Art. 38a BDSG; § 6 (4) AT DSG-2000);

g. von **Fachorganisationen** der bearbeitenden Stellen wie "privatim", VUD oder das Datenschutz-Forum schweiz diskutierte und erarbeitete Datenschutzgrundsätze;

h. Prüfung und Empfehlungen der Informationstätigkeit der bearbeitenden Stellen durch spezialisierte **Datenschutz-Beratungsunternehmen**.

A.6.4 Derartige Standards, Leitlinien und Verhaltensregeln in Form von "*Soft Law*" im Rahmen von *"Privacy Governance und Compliance*" eignen sich nach hier vertretener Auffassung wesentlich besser für den sachgerechten Umgang mit den aktuellen Anforderungen des Datenschutzes bei der rasch fortschreitenden "Digitalen Transformation" unseres Landes als ein komplexes Netzwerk administrativer Prüfungs-, Informations-, Melde- und Anzeigepflichten, welches sowohl die bearbeitenden Stellen als auch die personelle Infrastruktur des Beauftragten überlasten würde.

## B Stellungnahme zu ausgewählten Bestimmungen des RevE DSG

### Art. 1 Beschränkung des Datenschutzes auf natürliche Personen

/1 Während die Mehrheit der Begleitgruppe zur Revision des DSG vom 29. Oktober 2014 noch am bisherigen spezifisch schweizerischen Konzept der Geltung des DSG auch für juristische Personen festgehalten hat (Normkonzept zur Revision des Datenschutzgesetze Ziff. 4.2.1 https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf soll jetzt auf diesen (unechten, da bestehenden) *"Swiss Finish*" zur umfassenden Gewährleistung des Datenschutzes im öffentlichen und privaten Bereich verzichtet werden.

/2 Schon bei der Schaffung des DSG-1992 ist intensiv – unter Abwägung der dafür und dagegen sprechenden Argumente - über die Aufnahme der juristischen Personen in den Datenschutz diskutiert worden (Botschaft 88.032 vom23. März 1988, Ziff. 2.2.1 S. 438) "Juristische Personen" nach Art. 52 ff ZGB umfassen neben den gemäss Art. 552 ff OR als Handelsgesellschaften oder Genossenschaften organisierten wirtschaftlich tätigen grossen, mittleren und kleineren Unternehmen (wie erwähnt ca. 550'000 KMU's) sowie Einzelfirmen auch die "idealen Vereine", welche sich nach Art. 60 Abs. 1 ZGB einer "politischen, religiösen, wissenschaftlichen, künstlerischen, wohltätigen, geselligen oder anderen nicht wirtschaftlichen Aufgabe widmen" und die oft auf ähnliche Zwecke wie die Vereine ausgerichteten Stiftungen gemäss Art. 80 ff ZGB. Der Datenschutz schützt eben nach bisherigem Konzept eben nicht nur Grossfirmen mit internationaler Tätigkeit, sondern vor allem auch die Interessen von KMU's, Gewerbebetrieben, idealen Vereinen und Stiftungen mit oft philanthropischem Zweck.

/3 Die unter Ziff. 8.1.1.2 des Erläuternden Berichts zum Vorentwurf für die Totalrevision des Datenschutzgesetze https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Erl.-Bericht_de.pdf zum Ausschluss juristischer Personen aus dem Datenschutz abgegebene summarische Begründung "dieser Schutz sei in der Praxis nur von geringer Bedeutung und der Beauftragte habe zu diesem Bereich noch nie eine Empfehlung abgegeben" ist nicht überzeugend, genau so wie die Stellungnahme des Bundesrates vom 25.01. 2017 zur Motion von Claude Béglé vom 08.12.2016 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163963 Jedenfalls ist nach hier vertretener Auffassung das von den Verfassern des Erläuternden Berichts vorgebrachte Argument, man könne die juristischen Personen in Zukunft ohne Nachteil aus dem Schutzbereich des DSG ausschliessen, weil der Schutz ja durch Art. 13 BV sowie Art. 28 ZGB, die Sanktion von Persönlichkeitsverletzungen und die Gesetzgebung über die Fabrikations- und Geschäftsgeheimnisse gewährleistet sei, als etwas wagemutig zu betrachten. Mit dieser Argumentation könnte nämlich auch der Verzicht auf den Datenschutz überhaupt begründet werden. Tatsächlich wurde zu Beginn der Arbeiten an der Schaffung des DSG-92 die Idee diskutiert, ob man den sog. "Datenschutz" nicht aufgrund einer Idee des damaligen NR Andreas Gerwig (1928-2014) durch die Ergänzung von Art. 28 ZGB um zwei oder drei zusätzliche Absätze gewährleisten könne. Und wie durch den Ausschluss der juristischen Personen der Datenschutz in den übrigen Bereichen verbessert werden könnte ist unklar. Dieser doch recht kühne Schluss lässt sich jedenfalls dem zitierten Aufsatz von Christian Drechsler in AJP 1/2016 S. 85/86 nicht entnehmen.

/4 Das durch die Bundesverfassung (Art. 13 Abs. 2 BV) gewährleistete **Grundrecht jeder Person auf Schutz vor Missbrauch der sie betreffenden Daten** umfasst nach der Systematik der BV sowie des Personenrechts des ZGB (Art. 11) welche beide zwischen "Menschen" und "Personen" unterscheiden eindeutig auch körperschaftlich organisierte Personenverbindungen im Sinne von Art 52 ZGB. Diese sind bekanntlich gestützt Art. 53 ZGB aller Rechte und Pflichten fähig, die nicht die natürlichen Eigenschaften des Menschen ... zur notwendigen Voraussetzung haben (Ehrenzeller, St. Galler Kommentar zur Bundesverfassung 2.Auflage Rz 40 S. 325 und dort zit. BGE 95 II 481 und BGE 119 V 297). Grundrechte müssen ge-

mäss Art. 35 Abs. 1 BV in der ganzen Rechtsordnung zur Geltung kommen. Man könnte den Ausschluss juristischer Personen aus dem durch den RevE DSG vermittelten Rechtsschutz daher - etwas überspitzt - als "Verfassungsbruch" bezeichnen.

/5 Selbstverständlich wird durch das schweizerische Recht der Schutz der Persönlichkeit und der Privatsphäre auch der juristischen Personen in vielfältiger Weise gewährleistet: Niemandem wäre es bisher eingefallen, das **Fernmeldegeheimnis** (Art. 43 ff FMG und 321ter StGB) oder das Institut des **Bankkundengeheimnisses** (Art. 47 BankG), das **Geschäftsgeheimnis** (Art. 162 StGB; Art. 6 UWG), die Strafbarkeit des Einsatzes **von Abhör- und Aufnahmegeräten (**Art. 179bis ff StGB), die Verletzung des **Schriftgeheimnisses** (Art. 179 StGB) oder des **Amtsgeheimnisses** (Art. 320 StGB) auf natürliche Personen zu beschränken. Und Art. 28 ZGB als zivilrechtliche und über das vergleichbare europäische Recht hinausgehende Grundlage des Schutzes der Persönlichkeit kann auch von juristischen Personen angerufen werden: BGE 95 II 481 "Club Méditerranée" http://www.servat.unibe.ch/dfr/c2095481.html Daher bestehen nach hier vertretener Auffassung gute Gründe dafür, den in der Schweiz im Vergleich zu den umgebenden Staaten gut ausgebauten Schutz der Persönlichkeit, der Geschäftsgeheimnisse, des Bankkundengeheimnisses und des Datenschutzes, im Zivil-, Straf- und Verfahrensrechts als **Standortvorteil unseres Landes** zu betrachten. Es ist wohl kein Zufall, dass neben Österreich auch das Fürstentum Liechtenstein den Datenschutz juristischer Personen anerkennt. Jedenfalls würde ein international tätiges Unternehmen, wenn der Standort des Servers für die Speicherung wichtiger Geschäftsdaten in Deutschland, Frankreich, oder der Schweiz zu prüfen ist, wohl unserem Land den Vorzug geben.

/6 Bekanntlich werden juristische Personen durch ihre **Organe** (Art. 55 OR) bzw. durch ihre **handelsrechtlichen Vertreter tätig** (Art. 458ff und 717 OR), d.h. durch das Handeln natürlicher Personen: Im Handeln juristischer Personen schwingt in der Regel eine Tätigkeit natürlicher Personen mit. Im Einzelfall ist es daher nicht einfach, eine ausschliesslich auf eine juristische Person beschränkte Datenbearbeitung zu erkennen. Beispiel: Der typische Fall der Bestellung von Gütern bei einem Zulieferanten durch den Einkaufschef des Bestellers. Für Unternehmen ist die Möglichkeit der digitalen Signatur der von den physischen Vertretern unabhängigen elektronischen Signtur erst seit dem 1. Januar 2017 mit der Revision des Bundesgesetzes über die digitale Signatur vom 18. März 2016 durch die sog. "geregelte Signatur" gemäss Art. 7 ZertES ermöglicht worden. Es ist daher nach hier vertretener Auffassung eine **trügerische Hoffnung davon auszugehen, durch die Ausschaltung der juristischen Personen aus dem Rev DSG werde dessen Anwendung in der Praxis erleichtert**. Jedenfalls wäre in Zukunft von Fall zu Fall zu prüfen, ob in der Kommunikation mit einem Unternehmen, einem Verein oder einer Stiftung auch Angaben über deren er Organe oder geschäftlichen Vertreter enthalten sind, welche die betreffende Kommunikation dem Datenschutz unterstellt auch wenn unter dem RevE DSG den juristischen Personen der Datenschutz entzogen werden sollte.(in Deutschland spricht man in solchen Fällen von einem "datenschutzrechtlichem Durchgriff). Die echten Probleme, die sich aus der Anwendung des DSG auf juristische Personen ergeben, können jedenfalls kaum damit gelöst werden, dass

man den Datenschutz für juristische Personen einfach aufgibt. Vielmehr werden sich zahlreiche Zweifelsfälle ergeben, ob die alltägliche Kommunikation (durch Brief, Telefax oder E-Mail) mit dem Vertreter einer juristischen Person in den Anwendungsbereich des Datenschutzes (und damit dem Auskunfts- und Einsichtsrecht) fällt oder nicht. Darüber hinaus werden auch die **kantonalen Datenschutzgesetze**, welche ebenfalls den Schutz juristischer Personen kennen, dem neuen Rechtzustand anzugleichen sein.

/7 Im Weiteren ergibt sich entgegen den Ausführungen im Begleitbericht über die Rechtsentwicklung im europäischen Ausland dass dem Datenschutz für juristische Personen zunehmend Aufmerksamkeit geschenkt wird (Vgl. den Bericht von RA Dr. S. Kraska, externer Datenschutzbeauftragter betreffend die "Ausweitung der Datenschutzgesetze auf Daten juristischer Personen". https://www.iitr.de/veroeffentlichungen-des-instituts-fuer-it-recht/251-ausweitung-der-datenschutz-gesetze-auf-daten-juristischer-personen.html Nach dem Urteil des Europäischen Gerichtshofs ("EuGH") vom 6. November 2003 in der Rechtssache C-101/01 Bodil Lindqvist, Rz 98 schliesst die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten die Anwendung auf die von der erwähnten Richtlinie nicht erfassten Bereiche (scil. der juristischen Personen) nicht aus http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30d5513415265d354b44acf0cdb51683484b.e34KaxiLc3qMb40Rch0SaxyLaxn0?text=&docid=48382&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=332203 Auch das neuere Urteil des Verfassungsgerichtshofs des Bundeslandes Rheinland-Pfalz vom 13.05.2o14 VGH B 35/12 kommt zum gleichen Schluss: *"Der durch die rheinland-pfälzische Landesverfassung gewährleistete* ***Datenschutz ist nicht auf natürliche Personen beschränkt****. Auch juristische Personen und Personengesellschaften können sich vielmehr hierauf berufen, soweit die staatliche informationelle Maßnahme ihre spezifische Freiheitsausübung, d. h. insbesondere ihre wirtschaftliche Tätigkeit, gefährdet.*" https://www.rdv-online.com/aktuelles/datenschutz-nicht-auf-natuerliche-personen-beschraenkt Vgl. dazu auch den Bericht in RDV Online vom16.05.2014 "Datenschutz nicht auf natürliche Personen beschränkt" https://www.rdv-online.com/aktuelles/datenschutz-nicht-auf-natuerliche-personen-beschraenkt

/8 Die recht dürftigen Begründungen im Erläuternden Bericht für den Ausschluss juristischer Personen aus dem Geltungsbereich des Datenschutzes übersehen nach hier vertretenen Auffassung folgende wichtigen Aspekte des Datenschutzes in der Unternehmenspraxis:

a. Das elementare Recht auf **Auskunft und Zugang** zu den über eine juristische Person (Verein, Stiftung, Gesellschaft) **im privaten und öffentlichen Bereich** vorhandenen Daten gemäss Art. 8 DSG 1992/2006. Es gibt im Privatrecht k e i n allgemeines Recht auf Auskunft und Zugang zu den eine juristische Person betreffenden Daten. Schon bei der Ausarbeitung des DSG-1992 wurde erkannt, dass n i c h t der durch Art. 28 ZGB und vergleichbare Vorschriften der Rechtsordnung gewährleistete Schutz der Privatsphäre die Grundlage des Datenschutzes ausmacht, sondern das **Auskunftsrecht** (Dieses ist "**das bedeutendste Institut des Datenschutzes"** (Botschaft 88.032 vom23. März 1988, Art. 452-53). Im Auskunftsrecht kommt eben das zum ersten Mal im Urteil des deutschen Bundesverfassungsgerichts vom 15. Dezember 1983 betreffend den sog. "Mikrozensus" um-

schriebene "Grundrecht der informationellen Selbstbestimmung" https://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf zum Tragen, welches durch die ständige Praxis unseres Bundesgerichts bestätigt worden ist (statt vieler BGE 127 III 481; 138 II 346 Erw. 8.2).

b. Demgegenüber ist der Zugang zu amtlichen Akten nach dem "**Öffentlichkeitsprinzip**" (BGÖ -SR 152.3) und vielen kantonalen Gesetzen **durch zahlreiche Ausnahmen gekennzeichnet** (Art. 3-4 sowie Art. 7-8 BGÖ), welche über die Einschränkungen nach Art. 9 DSG weit hinausgehen Das Zugangsrecht nach BGÖ ist grundsätzlich am Ort der betreffenden Behörde durch Einsicht in die Akten geltend auszuüben und muss anders als das Auskunftsrecht nach Art. 8 DSG in einem kontradiktorischen Verfahren geltend gemacht werden, was aufgrund persönlicher Erfahrungen des Unterzeichnenden aufwändige Auseinandersetzungen mit der Verwaltung und dem Inhaber der betreffenden Akten viele Monate in Anspruch nehmen kann. Gerade die aktuelle Auseinandersetzung über die Einschränkung der Öffentlichkeit von Ausschreibungen des Bundes, welche weit herum als Skandal betrachtet wird, zeigt, auf welch dünnem Boden sich Unternehmen und Privatpersonen bewegen, wenn sie Zugang zu Daten der Verwaltung über das BGÖ erhalten möchten http://www.derbund.ch/schweiz/standard/beschaffungen-als-geheimsache-rueckschritt-in-die-steinzeit/story/16363986 Das Zugangsrecht nach dem BGÖ kann somit das Auskunftsrecht nach Art. 8 DSG-92/Art. 20-22 RevE DSG nicht ersetzen.

c. Die **Grundsätze über die Bearbeitung von personenbezogene Daten** unter dem Datenschutzgesetz (Art. 4 DSG) wie Treu und Glauben, Verhältnismässigkeit und vor allem die **Transparenz** haben in der Praxis auch für Vereine, Stiftungen und Handelsgesellschaften eine erhebliche Bedeutung. Insbesondere trifft dies auch für das "**Legalitätsprinzip**" nach Art. 27 RevE DSG für Bearbeitung von Daten über juristische Personen durch die (Bundes-)Verwaltung zu: Auch für die **Bearbeitung von Daten über juristische Personen** sollte weiterhin, auch nach der Revision des DG, eine **ausreichende Rechtsgrundlage** vorhanden sein.

/9 Aufgrund der praktischen Erfahrungen des Unterzeichnenden als Rechtskonsulent eines international tätigen Konzerns [welchem neulich seitens grosser Geschäftsbanken zugemutet wurde, im Hinblick auf die Auslagerung der Datenverarbeitung ins kostengünstige Ausland bei der Abwicklung von Bankgeschäften für sich und seine Kunden und Geschäftspartner auf den Schutz des Bankkundengeheimnisses zu verzichten!] ist die Vermutung nicht auszuschliessen, dass es mit dem Verzicht des Datenschutzes für juristische Personen nicht zuletzt darum gehen könnte, nach der weitgehenden Durchbrechung des lästig gewordenen Bankkundengeheimnisses eine weitere störende Auflage zum Schutz der Kunden im Geschäftsverkehr abzubauen.

/10 Andererseits verstehen wir - wiederum aufgrund unserer praktischen Erfahrungen in einem international tätigen Konzern - die Besorgnisse jener Kreise welche die sich aus der integralen Anwendung des Datenschutzes ergebenden auf juristische Personen ergebenden Probleme, insbesondere bei der Auslandbekanntgabe, durch die Ausklammerung der juristi-

schen Personen aus dem Schutzbereich des DSG lösen möchten, also das Kind mit dem Bad ausschütten möchten. Dabei wurde nach der persönlichen Erinnerung des Unterzeichnenden das Problem der Einbeziehung juristischer Personen in den Datenschutz, insbesondere bei Auslandbekanntgaben, schon bei der Schaffung des DSG in den 80er Jahren erkannt, dafür jedoch in jenem Zeitraum angesichts der noch wenig globalisierten Wirtschaft keine Lösungsmöglichkeiten entwickelt. Dabei würden auch nach dem harmonisierten europäischen Datenschutzrecht rechts- und verfassungskonforme Lösungsmöglichkeiten zur Verfügung stehen, indem bestimmte Pflichten der Verantwortlichen und Auftragsbearbeiten sowie die Rechte der betroffenen Personen auf die Bearbeitung von Daten über natürliche Personen beschränkt werden. Dabei ginge es einerseits darum, den durch die Gewährleistung des Datenschutzes für juristische Personen geschaffenen Standortortvorteil für unser Land im internationalen wirtschaftlichen Wettbewerb zu erhalten, andererseits die durch die Erhaltung des Datenschutzes für juristische Personen geschaffenen Auflagen für Verantwortliche und Auftragsbearbeiter, insbesondere bei der grenzüberschreitenden Datenbearbeitung auszuschalten bzw. nach Möglichkeit einzuschränken, also wie im Mühlespiel die Situation einer sog "Zwickmühle" herbeizuführen, welch es erlaubt, das Bestmögliche aus den gegebenen Umständen herauszuholen.

Formulierungsvorschläge zum Geltungsbereich

- Art. 1 RevE DSG "**natürliche" streichen**;
- Art. 2 Abs. 2 RevE DSG "**natürlicher" streichen**. Vorschlag für einen neuen Unterabsatz 2: "Das Gesetz gilt insoweit für die Bearbeitung von Daten juristischer Personen, als der Geltungsbereich nicht auf natürliche Personen beschränkt ist".
- Art. 3 RevE DSG "**natürliche oder juristische**" Person über die Daten bearbeitet werden.
- Art. 5 RevE DSG Titel "**Bekanntgabe der Daten natürlicher Personen ins Ausland**". Damit wäre die weltweite Bekanntgabe von Daten über juristische Personen frei - wäre allerdings mit dem Problem belastet, dass auch KMU, Einzelfirmen, Vereine und Stiftungen vom Datenschutz bei Auslandbekanntgaben vollständig ausgeschlossen wären. Diesbezüglich kann auf die weiteren Formulierungsvorschläge zu Art. 5 RevE DSG verwiesen werden.
- Art. 13 RevE DSG Titel: "**Informationspflicht bei der Beschaffung von Daten über natürliche Personen"** Die Ausdehnung dieser Informationsplicht auf juristische Personen dürfte im Geschäftsleben nach hier vertretener Auffassung zu einer unnötigen und nicht zielführenden Belastung der Verantwortlichen führen.
- Art. 15 RevE DSG: Kann man u.E. belassen, da **automatisierte Einzelentscheidungen**, z.B. über die Gewährung oder Verweigerung eines Kredits, eines Vertragsabschlusses oder einer Versicherung auch für juristische Personen, insbesondere KMU relevant sein können.
- Art. 16 RevE DSG: **Datenschutz-Folgeabschätzung** beschränken auf " .. Persönlichkeit oder die Grundrechte natürlicher Personen ... "

- Art. 17 REVE DSG: Die **Meldepflicht einer Datenschutz-Verletzungen** kann in jenen Fällen auch für juristische Personen relevant sein, wenn ihre Geschäftsdaten verloren gehen! Daher könnte diese Regelung auch für juristische Personen stehen bleiben
- Art. 19 Bst. b RevE DSG Diese **Informationspflicht** könnte uf Daten über natürliche Personen beschränkt werden
- Art. 24 Abs. 2 RevE DSG Zusätzlich wäre folgender neuer Rechtfertigungsgrund aufzunehmen, der unter den Experten schon bei der Schaffung des DSG-92 diskutiert worden ist

  " ... Daten über gewerblich tätige juristische Personen im Rahmen ihres Geschäftszwecks bearbeitet "

Das ist auf den ersten Blick eine recht lange Liste von Ausnahmebestimmungen, die sich jedoch auf Hinzufügung einzelner Wörter beschränkt. Dadurch soll ermöglicht werden, den sich aus der Anwendbarkeit des Datenschutzes auf juristische Personen ergebenden Standortvorteil der Schweiz im internationalen Wettbewerb (z.B. Bearbeitung von Daten ausländischer Unternehmen in einer in der Schweiz betriebenen "Cloud") zu erhalten, ohne dadurch für Verantwortliche und Auftragsbearbeiter aufgrund der im RevE DSG vorgesehenen verschiedenen neuen Pflichten unzumutbare Aufwendungen zu verursachen.

**Art. 2 Abs. 3 RevE DSG Ausnahmen vom Datenschutz**

Formulierungsvorschlag

Art. 2 Abs. 3 RevE DSG Ersatzlos streichen und die geltende Regelung beibehalten:

Das Verfahrensrecht stellt nach hier vertretener Auffassung "bereichsspezifisches Datenschutzrecht" dar. Die Ausübung von Ansprüchen aus dem Datenschutz (Auskunft und Einsicht, Sperre oder Löschung von Daten) in einem laufenden Verfahren würde zum Missbrauch der Institution geradezu herausfordern (Anspruch auf Löschung der Eingabe meines Prozessgegners?!)

**Art. 3 RevE DSG Begriffe**

**Bst. b/c** Man kann diese beiden Kategorien in einem Buchstaben zusammenfassen. Art. 9 (1) DSGVO ist diesbezüglich nicht ganz eindeutig. Aber auch bei den genetischen Daten wird es immer um Daten über natürliche Personen, nicht um jene eines Schimpansen oder eines Rassenpferdes gehen (obwohl neuerdings auch ein "Persönlichkeitsrecht von Tieren" diskutiert wird http://www.berliner-zeitung.de/wissen/persoenlichkeitsrecht--auch-tiere-sind-personen--3053128 ) , und die Kriterien von "genetisch" und "biometrisch" stimmen u.E. insofern überein.

Formulierungsvorschlag:

"genetische oder biometrische Daten, die eine natürliche Person eindeutig identifizieren"

**Art. 3 Bst f) RevE DSG Profiling**

Dies ist ein Beispiel, wo der "*Swiss Finish*" über die Regelung der DSGVO und der Datenschutzkonvention des Europarates unnötigerweise hinausgeht, indem (a) auch **manuelle Auswertungen** sowie (b) die Analyse **nicht personenbezogener Daten** als Grundlage für Profiling dienen soll.

Formulierungsvorschlag (in Anlehnung an die DSGVO und das geltende Recht, Art. 3 d DSG-92: Das Problem der durch die Aggregierung nicht besonders schützenswerter Daten geschaffenen "Persönlichkeitsprofile" wurde in unserem Land nämlich schon in den 80er Jahren erkannt!)

" Jede Art der automatisierten Bearbeitung von Daten über natürliche Personen, welche die Beurteilung wesentlicher Merkmale ihrer Persönlichkeit erlaubt "

**Art. 4 Datenschutzgrundsätze**

**Abs. 3** Die Beifügung des Begriffs "klar" schafft gerade keine Klärung sondern unnötige Abgrenzungsprobleme. Wie soll ein KMU beurteilen, ob der Zweck für eine betroffene Person "klar" erkennbar war. Es ist im Zweifel Sache des Richters, zu entscheiden, ob der Beschaffungszweck ausreichend deutlich angegeben worden ist.

Formulierungsvorschlag

"klar" ist zu streichen.

**Abs. 5** führt die bestehende Regelung von Art. 5 DSG-92 in Art. 4 RevE DSG über, was sachlich richtig ist. Hingegen schiesst die schon heute geforderte Pflicht zur "**Vernichtung**" unvollständiger oder nicht aktueller Daten, d.h. nicht nachgeführter Daten über das Ziel hinaus. Es wird übersehen, dass es sich bei den in Wirtschaft und Verwaltung vorhandenen Daten in einem erheblichen Umfang um **Archiv- oder Sicherungsdaten** handelt. Solche Daten dürfen - und können oft aus IT technischen Gründen - nicht einfach "vernichtet" d.h. aus einem Datenbestand entfernt werden, wenn sie nicht mehr vollständig oder nicht nachgeführt sind. Hingegen ist vorzusehen, dass sie zu vernichten oder für für die weitere Bearbeitung zu **sperren** sind.

Formulierungsvorschlag

" Andernfalls sind die Daten zu vernichten oder für die weitere Bearbeitung zu sperren. "

**Abs. 6 Satz 1 und 2**

Die Verwendung der Begriffe "eindeutig" und ausdrücklich" im gleichen Unterabsatz führt zu schwer auflösbaren Interpretationsproblemen, vor allem für die hunderttausende dem DSG unterstellten KMU's. Nach hier vertretener Auffassung ist für die im **ersten Satz** umschriebene Situation ein **"Opting-out"** zugelassen, während der **zweite Satz ein "Opting-in**" erfordert.

Formulierungsvorschlag

Im ersten Satz ist "eindeutig" ersatzlos zu streichen.

**Art. 5 RevE DSG Bekanntgabe ins Ausland**

Zweifellos eine der heikelsten Regelungen im Zeitalter der umfassenden Digitalisierung der Informations- und Kommunikationsvorgänge sowie des Zusammenwachsens des internationalen Wirtschaftslebens, wobei noch heute – und für die voraussehbare Zukunft - **die allermeisten Staaten und Wirtschaftspartner ausserhalb des EWR kein mit dem harmonisierten europäischen Datenschutzrechts vergleichbares Datenschutzniveau erreichen**. Angesichts der sehr grossen und ständig wachsenden Ströme von Waren und Dienstleistungen und des damit verbundenen Informationsverkehrs stehen wir hier vor dem bereits diskutierten **Mengenproblem**. Not tut nicht eine Regelung, welche Garantien, komplexe Prüf- und Informationspflichten umfasst, sondern vor allem auch die Schaffung einer Möglichkeit, dass **triviale Auslandbekanntgabe im alltäglichen Verkehr der globalen Arbeits- und Freizeitgesellschaft von den Anforderungen der Art. 5 und 6 RevE DSG ausgenommen werden**. Die Beschränkung von Art. 5 auf natürliche Personen wurde bereits im Zusammenhang mit dem Geltungsbereich erwähnt.

Formulierung - Eventual-Ergänzung 1: Insbesondere für den Fall, dass Daten en über juristische Personen von der Regelung der Auslandbekanntgabe nicht überhaupt ausgenommen werden. Unter Art. 5 Abs. 1 RevE DSG könnte angefügt werden.

" Die Auslandbekanntgabe von Daten über gewerblich tätige juristische Personen im Rahmen ihres Geschäftszwecks führt im Allgemeinen nicht zu einer Gefährdung der Persönlichkeit ".

Formulierung - Eventual-Ergänzung 2: Art. 5 Abs. 1 oder Abs. 7 RevE DSG könnte angesichts des Mengenproblems um folgende Bestimmung ergänzt werden

" Der Bundesrat umschreibt die Umstände bei deren Vorliegen im Regelfall nicht mit einer schwerwiegenden Gefährdung der Persönlichkeit betroffener Personen zu rechnen ist."

Denn wir haben es in Art. 5 nicht nur mit dem Problem des internationalen geschäftlichen Datenverkehrs zu tun, sondern mit dem **Mengenproblem** der abertausenden von Verantwortlichen und Auftragsbearbeitenden in unserem Land: In Übereinstimmung mit den Ausführungen von RA Ch. Drechsler in AJP 1/2016 S. 85/86 sollte das DSG auf jene kritischen Bereiche des Datenschutzes ausgerichtet und triviale Vorgänge ausgeklammert, wo im Regelfall nicht mit einer Gefährdung der Persönlichkeit oder der Grundrechte betroffener Personen zu rechnen ist, analog der Ausnahmeregelungen zur Registrierung von Datensammlungen unter Art. 4 und Art. 18 VDSG.

**Abs. 2**: Dieser Absatz könnte wie folgt ergänzt werden:

" Er (scil. der Bundesrat) berücksichtigt dabei die von internationalen Organisationen [scil. Angemessenheitsbeschluss nach Art. 45 DSGVO] getroffenen Feststellungen [scil. über die Angemessenheit in einem bestimmten Staat] sowie die Zugehörigkeit des betreffenden Staates zu einem völkerrechtlichen Vertrag über den Datenschutz [scil. modernisierte Datenschutzkonvention SEV 108 des Europarates]

**Abs. 3 Bst. b) und c)** und die damit verbundenen, gemäss Art. 50 RevE DSG erst noch mit Strafe bedrohten Melde- und Prüfverfahren sind in der Praxis, insbesondere für KMU's kaum umsetzbar

und führen zu einem voraussehbaren Vollzugsdefizit, das gemäss den Überlegungen von RA Ch. Drechsler in AJP 172016 S. 85/86 bei der Revision des DSG nach Möglichkeit zu vermeiden ist. Bst. b) und c) sollten zusammengefasst durch die nachstehende Regelung ersetzt werden, wobei dringend zu empfehlen ist, dass sich der Beauftragte an internationale Standards, Muster und Empfehlungen halten wird

Formulierungsvorschlag

"b) Garantien durch einen vom Beauftragten anerkannten standarisierten Vertrag oder vom Beauftragten empfohlene Vertragsklauseln; der Beauftragte berücksichtigt dabei internationale Standards und Empfehlungen" [scil. Art. 46 DSGVO]

Damit verbleben bleiben unter Abs. 3 als Voraussetzungen des Datenschutzes bei Auslandbekanntgaben in ein Land ohne angemessenen (Daten-)Schutz nur noch die Garantien gemäss Bst. a, b) und d), das zweifellos der Vereinfachung der Regelung durch Befreiung von administrativem Ballast dient.

**Abs. 4 - 6**

Formulierungsvorschlag

Die strafbewehrten Informations-, Melde- Prüf- und Genehmigungspflichten in Abs. 4-6 sind ersatzlos zu streichen.

Diese umständlichen und zeitraubenden Verfahren für die grenzüberschreitende Bekanntgabe sind in Art. 46 DSGVO nicht vorgesehen und qualifizieren als "*Swiss Finish*". Im Gegenteil wird in Art. 46 (2) DSGVO festgehalten, dass die standardisierten vertraglichen Garantien **ohne Genehmigung der Aufsichtsbehörde** verwendet werden können.

Die Aufrechterhaltung dieser administrativen Informations-, Melde- Prüf- und Genehmigungspflichten führt entweder zu einem massiven **Vollzugsdefizt** mit hypothetischer Strafbarkeit aller Unternehmen (insbesondere KMU) mit Geschäftskontakten ausserhalb des EWR, bzw. bei rechtskonformer Einhaltung dieser administrativen Auflagen zur Überlastung der Infrastruktur des EDÖB und auf jeden Fall zu einem erheblichen Nachteil der Schweizer Unternehmen im internationalen wirtschaftlichen Wettbewerb, ohne dass durch diese umfangreichen administrativen Massnahmen der Datenschutz relevant gefördert werden kann.

Es war und ist Sache der Verantwortlichen, die Pflichten des DSG über die Auslandbekanntgabe einzuhalten und sich im Zweifel um die Zulässigkeit einer Auslandbekanntgabe an den EDÖB zu wenden und sich von diesem gemäss Art. 41 Abs 4 RevE DSG beraten zu lassen.

**Art. 6 RevE DSG Bekanntgabe ins Ausland in Ausnahmefällen**

Im Sinne der Gewährleistung der praktischen Umsetzung des Datenschutzes und der Vermeidung von Vollzugsdefiziten ist diese Regelung wie folgt anzupassen:

**Abs. 1**

Formulierungsvorschläge

a) "... im Einzelfall ..." ist zu streichen bzw. zu präzisieren " im Einzelfall oder für eine Kategorie gleichartiger Bekanntgaben eingewilligt hat. In der Praxis, z.B. in einem bestehenden Lieferungsverhältnis, bei der Abwicklung von Ferienbuchungen u.ä. kommt es regelmässig zu zahreichen gleichartigen Bekanntgaben.

b) In Anlehnung an die erheblich praxisnähere Regelung von Art. 49 (1) b) DSGVO und zur Korrektur der durch die Einwirkung Aussenstehender auf die von der damaligen Expertenkommission erarbeiteten Fassung des DSG-92 der sollte Bst. b) wie folgt formuliert werden:

" b. die Bekanntgabe sich auf Daten des Vertragspartners im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages mit dem Vertragspartner sowie auf die Durchführung vorvertraglicher Massnahmen bezieht; "

c) Diese Bestimmung sollte in Anlehnung an die erheblich praxisnähere Regelung von Art. 49 (1) Bst. e DSGVO wie folgt umformuliert werden:

" c. Die Bekanntgabe erforderlich ist für

1. Die Wahrung eines überwiegenden öffentlichen Intereses, oder
2. Die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen "

**Abs. 2**

Diese Informationspflicht ist wie die vergleichbare Regelung unter Art. 5 RevE DSG **ersatzlos zu streichen**. Sie bringt ausser einem erheblichen administrativen Aufwand für Verantwortliche und den Beauftragten keine erhebliche Stärkung des Datenschutzes. Sie ist Teil des unter dem Aspekt der Harmonisierung mit dem europäischen Datenschutzrecht abzulehnenden überschiessenden *"Swiss Finish*", denn sie in Art. 49 DSGVO nicht vorgesehen.

**Art. 7 RevE DSG Auftragsdatenbearbeitung**

/1 Auftragsdatenbearbeitung ("*Outsourcing*") ist in der modernen Welt als arbeitsteiliges Zusammenwirken allgegenwärtig und deckt ein **sehr weites Feld von Bearbeitungsvorgängen** ab. Darunter fallen z.B. "*full service*" Lösungen der Beschaffung und Auswertung von personenbezogenen Informationen für ein bestimmtes Vorhaben wie z.B. eine Werbekampagne oder die Ermittlung der Kundenzufriedenheit, der Betrieb eines "*Call Centers"*, die Bearbeitung von Daten in Rechenzentren, auch durch Konzerngesellschaften, z.B. für die Auftragsabwicklung und Fakturierung oder die Personaladministration, die Erbringung von Service-Leistungen für die IKT Infrastruktur mit Zugang zu Personendaten, die Nutzung der Leistung von Grossrechnern für "Big Data Analysen" oder die externen Speicherung grosser Datenmengen. Dies gilt vor allem auch für unsere KMU's, die sich durch Auslagerung der Bearbeitung von Daten auf ihre Kerntätigkeit

konzentrieren können. Die Auftragsbearbeitung ist allerdings nach der Natur der Sache mit einem gewissen Risiko für die betroffenen Personen verbunden.

/2 Grundlage der Auftragsdatenbearbeitung ist immer ein **Vertrag** zwischen dem Verantwortlichen als Auftraggeber und dem Auftragsbearbeiter. Gegenstand, Inhalt und Umfang dieses Vertrages bestimmen sich im Bereich des Datenschutzes nach dem durch die Auslagerung von Personendaten geschaffenen Risiko für die betroffenen Personen. Für den Vertrag mit dem Auftragsbearbeiter sollte daher eine gewisse Form eingehalten werden, sonst wären gemäss Art. 1 OR auch mündliche oder sogar stillschweigend erteilte Aufträge zur Bearbeitung von Personendaten durch Dritte zulässig, deren Inhalt gar nicht nachgewiesen werden kann. So verlangt denn § 11 (1) BDSG ausdrücklich die Schriftform, übersieht jedoch offensichtlich die Möglichkeiten des online Abschlusses von Verträgen in der Informationsgesellschaft. Interessant ist nun, dass auch Art. 28 DSGVO nicht ausdrücklich die Schriftform für den Vertrag mit dem Auftragsbearbeiter fordert sondern die "Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten". Das bedeutet nach hier vertretener Auffassung, dass der Inhalt des Vertrages über die Auftragsdatenbearbeitung in Analogie zu Art. 358 ZPO und Art. 178 Abs. 1 IPRG **durch Text nachweisbar** sein sollte. vgl. dazu die Ausführungen im Urteil BGer 4A_618 / 2015 vom 09.03.2016 Ersw. 4.3 http://www.servat.unibe.ch/dfr/bger/160309_4A_618-2015.html

/3 Verantwortliche wie insbesondere KMU werden kaum über die Mittel und Kompetenzen verfügen um sich zu "vergewissern", dass der Auftragsbearbeiter die Datensicherheit und die Rechte der betroffenen Personen gewährleisten kann. Diese Anforderung wird auch durch Art. 28 (1) DSGVO nicht aufgestellt. Die entsprechende Pflicht des Verantwortlichen ist daher auf ein in der Praxis umsetzbares Mass zu beschränken.

/4 Der vom Auftragsbearbeiter einzuhaltende **Stand der Datensicherheit** ist bereits durch Art. 11 Abs. 1 RevE DSG umschrieben. Aus der Grundregel, dass der Auftragsbearbeiter die Daten nur so bearbeiten darf, wie der Verantwortliche es tun dürfte ergibt sich, dass der Stand der Datensicherheit beim Auftragsbearbeiter (mindestens) jenem des Verantwortlichen entsprechen muss.

/5 Die **ergänzende Rechtsetzungskompetenz** des Bundesrates für den Inhalt von Outsourcing-Verträgen ist mit Zurückhaltung zu beurteilen: Es handelt sich um einen aus Gründen des Datenschutzes nicht zwingend gebotenen **Eingriff in die Vertragsfreiheit** (Art. 19 OR). allerdings enthalten Art. 28 EU DSGVO, § 11 (2) BDSG und §§ 10/11 AT-DSG 2000 detaillierte Punktationen zum Inhalt des mit dem Auftragsbearbeiter abzuschliessenden Vertrages sowie zum Standard der Anforderungen an die Auftragsbearbeiter nach § 11 BDSG
https://www.gdd.de/downloads/materialien/ds-bvd-gdd-01/adv-standard

/6 Darüber hinaus gibt es verschiedene **Muster-Vereinbarungen**, wie jene des GDD Arbeitskreises "Datenschutz-Praxis": "Muster Auftrag nach § 11 BDSG" oder des Hessischen Datenschutzbeauftragten "Mustervereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen" https://www.bfdi.bund.de/bfdi_wiki/index.php/Mustervereinbarung_Auftragsdatenverarbeitung

Aber auch der EDÖB ist auf dem Gebiet der Auftragsdatenbearbeitung bereits mit Merkblättern und Empfehlungen tätig geworden, vgl. seine **Erläuterungen zum "Cloud Computing"**

https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de sowie die Herausgabe des mit zusammen mit der Wirtschaftskanzlei Homburger entwickelten **"Mustervertrages für das Outsourcing von Datenbearbeitungen ins Ausland**"
https://www.edoeb.admin.ch/datenschutz/00626/00743/00858/00859/index.html?lang=de

Ergänzend ist als Quelle für den Inhalt von Outsourcing-Verträgen auf das in Revision befindliche **finma Rundschreiben 17xx "Outsourcing – Banken und Versicherer**" hinzuweisen.

/7 Auf jeden Fall sollte sich der Bundesrat – auch angesichts der Vielfalt von Outsourcing-Situationen - darauf beschränken, in einer Art "Checklist" oder durch "Punktationen" die wesentlichen Anforderungen an den Inhalt eines Outsourcingvertrages zu umschreiben und dessen Aushandlung den Parteien zu überlassen. Er kann sich dabei an die Aufzählung der wesentliche Vertragspunkte in Art. 28 (3) DSGVO halten.

Formulierungsvorschlag

Aufgrund der vorstehenden Überlegungen wird folgender Vorschlag für Art. 7 RevE DSG formuliert:

" **Art.** 7 Auftragsdatenbearbeitung

1 Die Bearbeitung von Personendaten kann durch Gesetz oder Vereinbarung einem Auftragsbearbeiter übertragen werden, wenn ....

2 Der Auftragsbearbeiter muss hinreichende Garantien dafür bieten, dass er in der Lage ist, die Datensicherheit zu gewährleisten und die Rechte der betroffenen Personen zu wahren.

3 Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

4 Der Bundesrat umschreibt die wesentlichen Anforderungen an die Vereinbarung mit dem Auftragsbearbeiter.

5 Der Auftragsbearbeiter darf die Bearbeitung nur mit Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen.

6 Die Vereinbarung gemäss Abs. 1 sowie die Zustimmung nach Abs. 5 muss schriftlich oder in einer Form erklärt werden, welche den Nachweis durch Text ermöglicht. "

## Art. 8 RevE DSG Empfehlungen der guten Praxis

/1 "Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen" (sog. "**Deontologie**") in spezifischen Anwendungsbereichen waren bereits in Art. 27 der Richtlinie 95/46/EG vorgesehen, wurden in § 38a BDSG und § 6 (4) AT- DSG 2000 übernommen und sind nun in Art. 40/41 DSGVO geregelt.

/2 Art. 8 RevE-DSG umfasst **zwei deutlich von einander zu unterscheidende Arten von Verhaltensregeln**:

**A** ***Vom Beauftragten ausgearbeitete Empfehlungen***

Solche Empfehlungen sind eigentliche eine Erscheinungsform der in Art. 28 DSG-92 besonders hervorgehobenen **Beratungstätigkeit des Beauftragten**.

Der Beauftragte hat schon in der Vergangenheit eine ganze Reihe von Empfehlungen in der Form von "Merkblättern" oder "Leitfäden" erlassen, z.B. zur Bearbeitung von Personendaten am Arbeitsplatz, im medizinischen Bereich, zum Adresshandel, zur Überwachung des E-Mail und des Telefonverkehrs im Betrieb, zum Inhalt der Datenschutzerklärung im E-Commerce, zur Erhebung von Personendaten für Marketingzwecke, zur Videoüberwachung, über Anmeldeformulare für Mietwohnungen und viele andere.

Allerdings fehlte für solche Empfehlungen des Beauftragten zum Datenschutz in besonderen Anwendungsbereichen (sog. "bereichsspezifischer Datenschutz") bisher eine Rechtsgrundlage, und vor allem waren die Rechtswirkungen der Empfehlungen und deren Verbindlichkeit nicht klar geregelt. Auch ist und bleibt auch nach Art. 8 RevE DSG offen, wie vorzugehen ist, wenn sich der Beauftragte und die interessierten Kreise über den Inhalt einer Empfehlung nicht einigen können. U.E. darf der Beauftragte in einem solchen Fall die Empfehlung nicht erlassen, bzw. es sind die Konsultationen mit dem Beauftragten so lange fortzustzen, bis die Einigung über den Inhalt der betreffenden Empfehlung erreicht wird.

**B** ***Von Anwenderkreisen erarbeitete Verhaltensregeln***

Solche Empfehlungen, Standards, Code of Conduct existieren bereits in der Schweiz, z.B. jene der Schweizerischen Gesellschaft der Vertrauensärzte
https://www.vertrauensaerzte.ch/news/empfehlung.html

Es gibt aber auch verschiedene Selbstverpflichtungen zum Datenschutz von Schweizer Unternehmen oder Konzernen http://eligendo.ch/index.jsp?nodeId=95924 http://code-of-conduct.roche.com/de/datenschutz.html

Im Ausland ist als Anwendungsbeispiel auf den "Verhaltenskodex des Gesamtverbandes der Deutschen Versicherungswirtschaft ("GDV)" zu verweisen
http://www.gdv.de/2013/03/versicherungswirtschaft-und-datenschuetzer-schaffen-neue-massstaebe-fuer-datenschutz/

/4 Nach hier vertretener Aufforderung sind solche Verhaltensregeln mit einer Selbstverpflichtung zum Datenschutz ein wertvolles Instrument zur Umsetzung von Datenschutzvorschriften in einem bestimmten Anwendungsbereich. In den beiden vorstehend umschriebenen Fällen (A) und (B) sollten die Verhaltensregeln als **Kann-Vorschriften** ausgestaltet werden. Im Übrigen lehnt sich die vorgeschlagene Formulierung an Art. 40 / 41 DSGVO an

<u>Formulierungsvorschlag</u>

**Art. 8** Empfehlungen der guten Praxis

1 Der Beauftragte kann Empfehlungen der guten Praxis erarbeiten, welche die Datenschutzvorschriften in bestimmten Anwendungsbereichen konkretisieren. Er zieht dazu die inte-

ressierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs. [*Rest streichen, da redundant* ]

2 Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von Verantwortlichen oder Auftragsbearbeitern vertreten, können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Prüfung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie.

3 Der Beauftragte veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.

**Art. 9** Einhaltung der Empfehlungen der guten Praxis

Keine Bemerkungen – erscheint sachgerecht, denn der Datenschutz kann im Einzelfall auch eingehalten werden, wenn die Empfehlungen gemsäs Art. 8 RevEdSG nicht befolgt werden

**Art. 10 RevE DSG – Zertifizierung**

Keine Bemerkungen

**Art. 11 RevE DG Datensicherheit**

/1 Eigentlich ist es erstaunlich, dass die Vorschriften über die Datensicherheit ungeachtet der technologischen Entwicklungen und vielfältigen neuen Bedrohungen [Verbreitung von "Malware" über "Botnetze" oder "Drive-by-Download"; "Man-in-the-Middle" Attacken; "Advanced Persistent Threats" (APT); "Ransomware"; Unterdrückung des Gebrauchs der Informatik durch DDoS Attacken sowie Identitätsdiebstahl] im wesentlichen unverändert geblieben sind und das Bild der Bedrohung und der möglichen Gegenmassnahmen aus den 80er und frühen 90er Jahren wiedergeben.

/2 Andererseits spricht dies für die Technikneutralität der Formulierung von Art. 7 DSG-92 welche es erlaubt, auch neuartige Bedrohungen der Informatiksicherheit zu erfassen. Dennoch wird empfohlen, um dem Änderung des Bedrohungsbildes Rechnung zu tragen, die wichtigsten Risiken für die Sicherheit der Daten etwas konkreter zu umschreiben

/3 Im Weiteren wird vorgeschlagen in Anlehnung an Art. 8 VDSG und an die Entwicklung der internationale Gesetzgebung (§ 9 BDSG; § 14 AT-DSG 2000; Art. 32/33 DSGVO) die Kriterien für die Angemessenheit der technischen und organisatorischen Massnahmen näher zu umschreiben. Aufgrund ihrer grundsätzlichen Natur wird empfohlen, diese Anforderungen im Gesetz und nicht bloss auf Verordnungsstufe (bisher Art. 8 VDSG) festzuhalten. Dabei sollte in Anlehnung an Art. 32 (1) DSGVO zum Ausdruck kommen, dass die Datensicherheit nie absolut sondern nur nach Massgabe der Natur der Daten, der Bearbeitungsvorgänge, der Eintrittswahrscheinlichkeit eines "Datenunfalls" und der Schwere dessen Folgen sowie der Implementierungskosten gewährleistet

werden kann. Nach wie vor gilt der Ausspruch meines ehemaligen IBM Kollegen Prof. Dr. K. Nagel http://www.prof-nagel.de "Wer absolute (Daten-)Sicherheit sucht findet Verzweiflung!"

/4 Die Umschreibung der zahlreichen technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit, die aufgrund der Entwicklung der Bedrohungslage und dem Stand der Technik ständigen Änderungen unterworfen sein werden, sollte nicht dem Bundesrat, sondern im Sinne von Empfehlungen der guten Praxis nach Art. 8 Abs. 1 RevE DSG dem Beauftragten übertragen werden. Hingegen kann und soll dem Bundesrat die Aufgabe und die Kompetenz übertagewerden, die Mindestanforderungen an die Datensicherheit festzulegen. Er wird sich dabei an die geltenden internationalen Normen und Standards halten.

Formulierungsvorschlag

**Art. 11** Sicherheit von Personendaten

1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten.

2 Diese müssen durch technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten wie insbesondere unbeabsichtigte Veränderung, Vernichtung, Verlust, Missbrauch, Unterbrechung oder Verhinderung der Bearbeitung, Offenlegung oder unbefugten Zugriff geschützt werden.

3 Die technischen und organisatorischen Massnahmen müssen angemessen sein und insbesondere folgenden Kriterien Rechnung tragen

a. Zweck sowie Art und Umfang der Datenbearbeitung
b. Einschätzung der möglichen Risiken für die betroffenen Personen
c. gegenwärtiger Stand der Technik
d. Verhältnis des Aufwandes zum angestrebten Schutzzweck

4 Die Massnahmen sind periodisch zu überprüfen und erkannten neuen Bedrohungen anzupassen

5 Der Bundesrat legt unter Berücksichtigung international anerkannter Standards die Mindestanforderungen an die Datensicherheit fest.

**Art. 12 Daten einer verstorbenen Person**

Diese Bestimmung ist namentlich aus folgenden Gründen **ersatzlos zu streichen**

- Die Bestimmung ist ein besonders exotischer Ausdruck des *"Swiss Finish",* weil eine entsprechende Regelung im harmonisierten europäischen Datenschutzrecht nicht einmal ansatzweise vorhanden ist
- Sie ist dem Persönlichkeits- und Datenschutz fremd: Denn die Persönlichkeit und deren Schutz endet mit dem Tod der betroffenen Person (Art. 31 Abs. 1 ZGB): Ein Toter / Erblasser kann daher gar an seinen Personendaten gar k e i n e "überwiegenden Interessen" haben

- Warum nur die in direkter Linie mit der verstorbenen Person Verwandten und nur die im Zeitpunkt des Hinschieds des Verstorbenen mit ihm durch Ehe oder Partnerschaft verbundenen Personen Zugang zu den Daten des Verstorbenen haben sollen ist unklar
- Die Bestimmung ist nicht auf das Auskunftsrecht nach Art. 20-22 RevE DSG abgestimmt, insbesondere nicht auf ds Recht zur Auskunftsverweigerung nach Art. 21 RevE DSG
- Der Ausschluss des Amts- oder Berufsgeheimnisses (Spitalpersonal) ist nicht auf die prozessualen Verweigerungsgründe abgestimmt (Art. 231 StGB iVm Art. 166 ZPO)
- Eine Regelung über den Zugang zu Daten verstorbener Personen ist in Art. 1 Abs. 7 VDSG enthalten und könnte allenfalls noch ergänzt werden.

**Anstelle von Art. 12 RevE DSG Bezeichnung eines betrieblichen Datenschutzbeauftragten**

/1 Aufgrund der beruflichen Erfahrungen des Unterzeichnenden als Rechtskonsulent der IBM (Schweiz) und eines international tätigen Schweizer Konzerns (Alusuisse - Alcan - Rio Tinto), als Mitglied der Arbeitsgruppen des Bundes zur Schaffung des DSG-1992, als mehrjähriger geschäftsführender VR Präsident eines mittelständischen KMU, der Tätigkeit in verschiedenen Fachorganisationen (swissmem, swico, s-i, VUD, ISSS) sowie der Wahrnehmung von Lehrverpflichtungen bin ich der Überzeugung, dass die Bezeichnung eines betriebliche Datenschutzbeauftragten ("bDSB") eine **wesentliche Voraussetzung für die praktische Umsetzung des Datenschutzes** bei Verantwortlichen und Auftragsbearbeitern darstellt.

/2 Solche Beauftragte werden im schweizerischen Recht ja auch für andere risikoträchtige Tätigkeiten vorgesehen, wie Fachleute für die **Arbeitssicherheit und Gesundheitsschutz** http://www.ekas.admin.ch/index-de.php?frameset=29 in der **chemischen Industrie** https://berufsberatung.ch/dyn/show/1900?id=7201 oder als **Gefahrgutbeauftragte** für die Beförderung gefährlicher Güter auf Strasse, Schiene und Gewässern gemäss der Verordnung 741.622 https://www.admin.ch/opc/de/classified-compilation/20001699/index.html

/3 Die Umsetzung der Datenschutzvorschriften in Unternehmen und Verwaltung, v.a. aber bei Dienstleistungsbetrieben, welche sich im Rahmen ihrer Kerntätigkeit in erheblichem Umfange mit der Bearbeitung von Personendaten befassen setzt die Bezeichnung einer Person bzw. eines Stabes von speziell ausgebildeten Fachleuten, bzw. die Beauftragung eines externen Sachverständigen voraus welche die Geschäftsleitung bzw. die Linienfunktionen in der Anwendung des DSG beraten, die technischen und organisatorischen Massnahmen zur Umsetzung beantragen und für die Wahrnehmung der verschiedenen gesetzlichen Sorgfaltspflichten beim Umgang der Personendaten von angestellten, Kunden, Lieferanten und Geschäftspartnern sorgen können.

/4 Es ist daher schwer begreifbar, wie man bei der Vorbereitung der Totalrevision des DSG zur Auffassung kommen konnte eine Regelung der Bestellung eines bDSB im Gesetz sei entbehrlich. Dies kann eigentlich nur dadurch erklärt werden, dass die Verfasser des Gesetzesentwurfs relativ weit von den Realitäten der Umsetzung des Datenschutzes in der Praxis entfernt sind.

/5 Besonders befremdlich ist der Umstand dass Art. 37, 38 und 39 der DSGVO wie schon §§ 4 f) und g) BDSG die Benennung des bDSB, dessen Stellung und dessen Aufgaben ausführlich vorsehen. Und mit der im Rahmen der DSG Revision vom 24. März 2006 geschaffenen Möglichkeit der Bezeichnung eines bDSB (Art. 11a Abs. 5 Bst. e) DSG-2006) ergänzt durch die Regelungen in Art. 12a und 12b VDSG ist in der Schweiz eine Rechtsgrundlage für die schon vorher bei grossen Verantwortlichen und Auftragsbearbeitern eingesetzten bDSB geschaffen worden.

/6 Dies hat in der Folge zum Aufbau entsprechender **Vereinigungen von Datenschutz-Spezialisten** geführt wie der **VUD** Verein Unternehmensdatenschutz http://www.vud.ch das **Datenschutzforum** http://www.datenschutz-forum.ch/index.php?id_seite=20 sowie **privatim** die Vereinigung der öffentlich-rechtlichen Datenschutzbeauftragten der Kantone und verschiedener Gemeinden https://www.privatim.ch/de/datenschutzbeauftragte-kantone.html Im Ausland kann auf den 1989 gegründeten **Berufsverband der Datenschutzbeauftragten Deutschlands** (BvD) e.V. hingewiesen werden https://www.bvdnet.de/verband.html Es sind diese Organisationen, die neben dem Gesetzgeber, den Empfehlungen des Beauftragten sowie den Urteilen der Gerichte wesentlich zur Entwicklung und Implementierung des Datenschutzes in unseren Lande beigetragen haben.

/7 Wichtig ist nach hier vertretener Auffassung auch folgende Feststellung: Mit der Bezeichnung des bDSB sollen Verantwortliche und Auftragsbearbeiter von verschiedenen - z.T. mit Strafe bewehrten – administrativen Obliegenheit, insbesondere von Meldepflichten an den Beauftragten entlastet werden - aber auch der Beauftragte von der aufwändigen Entgegennahme, Prüfung und Genehmigung dieser Informationen: Dies ist administrativer Leerlauf der für den Datenschutz sehr wenig bringt. Die Bezeichnung des bDSB stellt nach hier vertretener Auffassung die Verlagerung von Aufsichtsfunktionen des Beauftragten in jene Betriebe dar, welche für den Datenschutz heikle Bearbeitungen durchführen. Dies entspricht einem Grundprinzip der schweizerischen Privatrechtsordnung: Wo immer möglich sollen nicht der Staat und seine Beamten für die Umsetzung von Rechtsvorschriften sorgen, sondern die dem Gesetz unterstellten Unternehmen durch interne Regelungen in Wahrnehmung ihrer Organisationsautonomie.

/8 Aufgrund dieser Überlegung wurde an erster Stelle den Grundsatz der Freiwilligkeit der Bezeichnung eines bDSB im privaten Bereich aufgestellt, weil damit Verantwortliche, Auftragsbearbeiter und der EDÖB mit seinem Stab von administrativen Aufgaben (Melde- Prüfungs- und Genehmigungspflichten) entlastet und ihrer Kernaufgabe der Umsetzung des Datenschutzes in Betrieb und Verwaltung zugeführt werden können. Es stellt sich andererseits die Frage, ob bei Vorhandensein bestimmter Situationen die Bezeichnung eines bDSB von Gesetzes wegen erforderlich ist. Dabei ist allerdings das eingangs erwähnte "Mengenproblem" zu berücksichtigen: Die Situationen, in denen die Bezeichnung des bDSB vom Gesetzt verlangt wird, sind so zu umschreiben, dass nicht jedes KMU und jeder Gewerbetreibende einen bDSB bezeichnen muss, sondern bDSB – unter Vorbehalt des Rechts auf freiwillige Einsetzung - nur dort bestellt werden, wo für den Schutz der Persönlichkeit und der Grundrechte betroffener Personen kritische Bearbeitungen von Personendaten durchgeführt werden.

Aus diesem Grund werden nachstehend **zwei Alternativen** für die Bezeichnung des bDSB zur Diskussion gestellt:

Formulierungsvorschlag 1 (mit Pflicht zur Einsetzung eines bDSB in qualifizierten Fällen)

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 gewerbsmässig Personendaten für Verantwortliche bearbeiten

c. Verantwortliche wenn sie

1 zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet sind oder wenn sie ohne gesetzliche Pflicht

2 regelmässig besonders schützenswerte Personendaten bearbeiten oder Profiling betreiben

3 als Teil ihrer gewerblichen Tätigkeit Personendaten nicht bei der betroffenen Person beschaffen

4 regelmässig Personendaten an Dritte und / oder ins Ausland bekanntgeben

5 regelmässig Entscheidungen über eine Vielzahl von 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 erlässt Bestimmungen über Stellung und Aufgaben des betrieblichen Datenschutzbeauftragten sowie zu den Ausnahmen von der Pflicht zur Bezeichnung eines betrieblichen Datenschutzbeauftragten.

Formulierungsvorschlag 2

1 Bundesorgane sind Bezeichnung eines Datenschutzbeauftragten verpflichtet wenn sie Personendaten bearbeiten

2 Verantwortliche und Auftragsbearbeiter können einen Datenschutzbeauftragten bezeichnen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und in den vom Gesetz umschriebenen Fällen die dem Verantwortlichen oder Auftragsbearbeiter übertragenen Prüf-, Melde- und Informationspflichten erfüllt und den Kontakt mit dem Beauftragten wahrnimmt.

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.

**Art. 13 / 14 RevE Informationspflicht und deren Ausnahmen**

/1 Die Verschaffung von Transparenz über die Bearbeitung von Personendaten ist ein zentrales Anliegen des Datenschutzes. Die Regelung nach Art. 13/14 RevE DSG ist allerdings so komplex und enthält verschiedene heikle Abgrenzungen dass sie für KMU's kaum rechtskonform umzusetzen ist. Es zeichnet sich einmal mehr ein von RA Ch. Drechsler in AJP 1/2016 befürchtet Vollzugs-Defizit ab.

/2 Darüber werden bei der Bestimmung von Art. 13/14 RevE DSG die Erwähnung wichtiger Grundsätze von Art. 12 DGVO vermisst, wie z.B. dass die den betroffenen Personen zu vermittelnden Informationen, wie heute üblich, nicht von Fall zu Fall mündlich oder schriftlich, auf einem festen Datenträger (Verpackung, Kundenkarte), sondern elektronisch (Datenschutzerklärung auf der Webseite eines Internehmens oder einer Verwaltungsstelle bzw. in elektronisch übermittelten AGB's) offenbart werden können.

/3 Nicht geregelt ist die Frage, ob und wie die Information bei späteren Änderungen der Bearbeitung zu erfolgen hat, z.B. wenn die Daten an weitere Dritten bekannt gegeben werden oder für "Big Data Analysen" genutzt werden, und in welcher Sprache eigentlich die Information, oder durch Bildsymbole (Art. 12 (8) DSGVO) zu erfolgen hat. Reicht es aus, wenn die Angaben über eine neue oder geänderte Bearbeitung im Zeitpunkt der Änderung der Bearbeitung auf der Webseite des Verantwortlichen publiziert werden?

**Art. 15 RevE DSG – Automatisierte Einzelentscheidungen**

Die Kombination der Begriffe "rechtliche Wirkung" mit "erhebliche Auswirkung" schafft eine gewisse Unklarheit, unter welchen Umständen die Informationspflicht zum Tragen kommt: Reicht irgendwelche rechtliche Wirkung aus, oder muss diese erhebliche Auswirkungen haben. Art. 22 (1) DSGVO ist in dieser Beziehung ein wenig, aber nicht viel! präziser.

**Art. 16 Rev. E DSG Datenschutz-Folgenabschätzung**

/1 Schon bisher haben Datenschutz-bewusste Anwender, vor allem wenn sie einen bDSB bezeichnet hatten, im Sinne einer "Datenschutz-Verträglichkeitsprüfung" bei neuen Anwendungen mit der Bearbeitung von Personendaten die Risiken für die Persönlichkeit der betroffenen Personen sowie die Einhaltung der Anforderungen aus den geltenden Datenschutzvorschriften

überprüft und die sich daraus ergebenden organisatorischen und technischen Massnahmen zur Gewährleistung des Datenschutzes intern dokumentiert. Voraussetzung einer Datenschutz-Folgenabschätzung sollte in Anlehnung an Art. 29 Abs. 1 Bst. a DSG 1992/2006 sein, dass die betreffende Bearbeitung geeignet ist, die Persönlichkeit einer grösseren Anzahl von betroffenen Personen zu verletzen: sog. "**Systemfehler**". Es geht einmal mehr darum, unter Berücksichtigung der Mengenproblematik aus der Masse der Bearbeitung von Personendaten jene (wenigen!) Situationen zu definieren, in welchen eine Folgenabschätzung durchzuführen ist.

/2 Die Durchführung der Datenschutz-Folgenabschätzung beruht auf der Beurteilung der Datenschutz-Risiken nach dem pflichtgemässen Ermessen der Verantwortlichen; diese werden im Sinne von Art. 35 (2) DSGVO den Rat eines von ihnen (gemäss dem neu vorgeschlagenen Art. 12 RevE DSG) bezeichneten bDSB einholen,

/3 Angesicht der sich stürmisch ausbreitenden Digitalisierung von Wirtschaft und Gesellschaft werden in Zukunft häufig Datenschutz-Folgenabschätzungen vorzunehmen sein. Damit tritt auch hier das wie schon mehrfach erwähnte **Mengenproblem** auf. Es besteht daher ein Bedürfnis der zur Durchführung einer Datenschutz-Folgenabschätzung Verpflichteten, dass Ihnen jemand - der Bundesrat in der Vollzugsgesetzgebung oder der Beauftragte durch Erlass einer Empfehlung im Verfahren nach Art. 8 RevE DSG - eine Anordnung betreffend die Fälle erteilt, in denen die Durchführung einer Datenschutz-Folgenabschätzung als erforderlich erachtet wird, ergänzt durch Angaben über deren Gegenstad, Inhalt und Struktur. Der Bundesrat oder der Beauftragte kann sich dabei an den Vorgaben von Art. 35 (3) und (7) DSGVO orientieren.

/4 Die Regelung in Art. 16 RevE DSG geht aufgrund der darin statuierten obligatorischen Melde- und Prüfungspflichten in Verbindung mit der Strafdrohung nach Art. 50/52 RevE DSG eindeutig über die Grundregel der Konsultationsmöglichkeit nach Art. 36 DSGVO hinaus, ist ein Beispiel des unbedingt zu vermeidenden "*Swiss Finish*" und würde notwendigerweise zu einem sehr hohen Aufwand der Anwender aber auch des Beauftragten und seines Stabes führen. Denn es wäre bei der vorgeschlagenen (zu) weit gefassten Formulierung von Art. 16 Rev EDSG mit hunderten oder tausenden von Folgenabschätzungen – oder aber mit einem massiven Vollzugsdefizit. zu rechnen. Es besteht daher ein **dringender Bedarf an der Entwicklung einer praxisgerechten Regelung.** Diese kann nach hier vertretener Auffassung nur in der Beschränkung der Pflicht zur Durchführung einer "Datenschutz-Folgenabschätzung" auf die Fälle eines qualifiziert erhöhten Risikos für die Persönlichkeit und die Grundrecht der betroffenen Personen bestehen.

/5 Darüber hinaus sollten die Ergebnisse der Datenschutz-Folgenabschätzung nicht dem Beauftragten einzureichen und von diesem zu prüfen sein, sondern von den **Verantwortlichen oder Auftragsbearbeitern dokumentiert und dem Beauftragten im Falle einer Prüfung vorgelegt werden.** Von der Berichts- und Informationspflicht nach Art. 16 Abs. 3 RevE DSG ist unbedingt abzusehen: Diese würde die personellen und materiellen Kapazitäten des Beauftragten und seines Stabes um ein Mehrfaches überschreiten und nach hier vertretener Auffassung zu einem eigentlichen "Vollzugs-Notstand" führen.

/6 In diesem Zusammenhang wird ferner beantragt, dass **Auftragsbearbeiter** grundsätzlich keine Folgenabschätzung durchzuführen haben: Denn sie werden im Auftrag und nach den Anweisungen des Verantwortlichen tätig und können das Risiko der ihnen übertragenen Bearbeitungshandlungen für die Persönlichkeit und die Grundrechte der betroffenen Personen im Regel-

fall überhaupt nicht beurteilen. Eine Datenschutz-Folgenabschätzug durch Auftragsbearbeiter käme nach hier vertretener Auffassung nur dann in Betracht, wenn sie im *"full service*" für ihren Auftraggeber Personendaten beschaffen, aufbereiten und auswerten.

/7 Es sollte jedoch auch die Möglichkeit geschaffen werden, dass Verantwortliche wie auch Auftragsbearbeiter, um sich gegen die Risiken einer Datenschutzverletzung abzusichern, die Dokumentation der vorgesehene Bearbeitung und der zu treffenden organisatorischen und technischen Massnahen dem Beauftragten unterbreiten können, welcher sich hierauf in einer kurzen Frist von einem Monat darüber aussprechen soll, ob er diese als genügend erachtet oder zusätzliche organisatorische und technische Massnahmen empfiehlt. Die Ergänzung, Anpassung und Konkretisierung der Datenschutz-Folgenabschätzung erfolgt hierauf in einem einvernehmlichen Verfahren zwischen dem Beauftragtem und dem Verantwortlichen bzw. Auftragsbearbeiter wie sich dies schon im geltenden Datenschutzrecht bewährt hat.

/8 Ein solches Verfahren lehnt sich an die Regelung von Art. 6 Abs. 5 VDSG an und ist **auch im** Wettbewerbsrecht (Art. 26 ff KG) bei **Vorabklärungen auf Begehren der Beteiligten** mit der Möglichkeit einvernehmlicher Regelungen (Art. 29 KG) vorgesehen, wo ebenfalls von einer 30-tägigen Antwortfrist der Behörde ausgegangen wird. Für ein solches "**Datenschutz-Ruling" des Beauftragten** in einem freiwilligen Verfahren besteht nach hier vertretener Auffassung ein erhebliches Interesse der Verantwortlichen und Auftragsbearbeiter.

/9 Es versteht sich im Weiteren von selbst, dass die ohnehin zweifelhaften **Strafbestimmungen** von Art. 50/51 RevE DSG dem angepassten Konzept der Datenschutz-Folgenabschätzung anzupassen sind. Die **Übergangsbestimmung** von Art. 59 Bst. a RevE DSG mit einer zweijährigen Übergangsfrist zur Herstellung der Bereitschaft für die Durchführung einer Datenschutz-Folgenabschätzung wird für sachgerecht gehalten. Allerdings ist aufgrund der Formulierung von Art. 59 a. RevE DSG nicht ganz klar, ob eine Datenschutz-Folgenabschätzung nach Ablauf der Frist von zwei Jahren auch für bereits bestehende Bearbeitungen durchzuführen ist; diese sollte nach hier vertretener Auffassung nur für neue oder erheblich geänderte Bearbeitungen in Frage kommen.

<u>Formulierungsvorschlag</u>

**Art. 16** Datenschutz-Folgeabschätzung

1 Führt eine vorgesehene Datenbearbeitung nach der Beurteilung des Verantwortlichen oder des Auftragsbearbeiters voraussichtlich zu einem erheblich erhöhten Risiko für die Persönlichkeit oder die Grundrechte einer grösseren Anzahl von betroffenen Personen, so ist vorgängig eine Datenschutz-Folgenabschätzung durchzuführen. Dabei ist der Rat des bezeichneten internen Datenschutzbeauftragten einzuholen.

2 Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen sowie die organisatorischen und technischen Massnahmen, die vorgesehen, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Personen zu verringern.

3 Im Falle der vorgesehenen Änderung des Bearbeitungsverfahrens ist die Datenschutz-Folgenabschätzung zu aktualisieren und anzupassen.

4 Die Datenschutz-Folgenabschätzung ist zu dokumentieren und dem Beauftragten im Rahmen einer Prüfung vorzulegen.

5 Die Verantwortlichen können die von Ihnen erstellte Datenschutz-Folgenabschätzung dem Beauftragten zur Prüfung vorlegen. Dieser teilt ihnen innert 30 Tagen nach Empfang der Information mit, wenn er eine Ergänzung oder Änderung der Datenschutz-Folgenabschätzung und der vorgeschlagenen organisatorischen und technischen Massnahmen empfiehlt.

6 Der Bundesrat erlässt Bestimmungen über die Fälle in denen eine Datenschutz-Folgenabschätzung durchzuführen ist, sowie über deren notwendigen Aufbau und Inhalt.

**Art. 17 RevE DSG Meldung von Verletzungen des Datenschutzes**

/1 Das Konzept der Pflicht zur Meldung von Datenschutz-Verletzungen, v.a. im Falle des Verlusts von Datenträgern mit gespeicherten Personendaten bzw. beim Abhandenkommen von Personendaten aufgrund von Hackerangriffen entstand in den US.A. (zunächst in Kalifornien "The California 2002 Data Security Breach Notification Law") und führte zu zahlreichen ähnlichen Erlassen zunächst in den U.S. Bundesstaaten

/2 Als Folge dieser Rechtsentwicklung kam es aufgrund von zu weit gehenden gesetzlichen Auflagen zu zahlreichen Meldungen in den Medien, z.B. über verlorene USB Sticks, Laptops. Mobiltelefone, was kaum etwas zum Schutz der Persönlichkeit der möglicherweise betroffenen Personen wohl aber zu deren Verunsicherung beigetragen hat. Dies ist ein Musterbeispiel der von einer an sich gut gemeinten Gesetzgebungsinitiative bewirkten "*unintended consequences*" (vgl. Robert Merton 1936 "The Unanticipated Consequences of Purposive Social Action").

/3 Die Meldepflicht bei Datenpannen hat sich hierauf auch im europäischen Datenschutzrecht ausgebreitet. Die Schaffung einer Meldepflicht wurde u.W. erstmals in der Richtlinie 2009/136/EG vom 25. November 2009 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation verankert. Später wurde die Meldepflicht mehr oder weniger unbesonnen in § 42a BDSG; § 24 (2) AT-DSG 2000 sowie Art. 33-34 DSGVO übernommen.

/4 Nach hier vertretener Auffassung erscheint die Pflicht zur Meldung von Verletzungen des Datenschutzes an die betroffenen Personen als eine in das Datenschutzrecht übernommene Ausprägung der allgemeinen Treue- und Sorgfaltspflicht sowie der Rechenschaftspflicht des Beauftragten bei der Ausführung von Arbeitsleistungen gemäss Art. 398 und 400 OR. Für den Zeitpunkt der Meldung an den Beauftragten bzw. die betroffenen Personen kann man sich a die Regelung für das Vorgehen bei Feststellung und Mitteilung der Mängelrüge nach Art. 201 und 367 OR anlehnen.

/5 Hingegen bringt die Meldung einer Datenschutzverletzung an den Beauftrgten für den Datenschutz eigentlich sehr wenig: Was soll der Beauftragte mit der Meldung anfangen, dass ein Arzt an einem Ärztekongress seinen Laptop mit elektronischen Krankengeschichten, ein Anwalt sein Mobiltelefon mit den Adressen von Klienten verloren hat, oder dass die Kundendatenbasis eines Versandhauses durch kriminelle Täter gehackt worden ist? Meldungen sind eigentlich nur für betroffene Personen von Bedeutung indem sie z,B. ihre Kreditkarte sperren oder eine andere

Mobiltelefonnummer erwerben können. Oder man denke an den Fall der Liechtensteiner LGT Bank https://de.wikipedia.org/wiki/Liechtensteiner_Steueraffäre welche vom Verkauf einer CD mit Kundendaten durch ihre ehemaligen Mitarbeiter Heinrich Kieber an die Bundesrepublik Deutschland zwar Kenntnis hatte, die betroffenen Kunden aber nicht rechtzeitig warnte, so dass diese in den umfangreichen Steuerstrafverfahren die Möglichkeit verloren haben, noch eine strafmindernde Selbstanzeige zu erheben.

/6 Mit der blossen Meldung von Datenschutzverletzungen sollte es daher nach hier vertretener Auffassung nicht getan sein: Vielmehr sollten Verantwortliche bzw. Auftragsbearbeiter im Sinne von Art. 44 OR die möglichen und verfügbaren organisatorischen und technischen Massnahmen ergreifen, um die Ursache der Datenschutzverletzung bzw. des Datenverlustes zu analysieren, künftige Verletzungen auszuschliessen oder in ihren Auswirkungen zu mindern. Dazu kann auch die Mitteilung der Datenschutzverletzung an Betroffene gehören, welche persönliche Schutzmassnahmen ergreifen können, wie die erwähnte Sperrung ihrer Kreditkarte oder ihres Mobiltelefons.

/7 Wenn ein Verantwortlicher einen betrieblichen Datenschutzbeauftragten bezeichnet hat, ist dieser nach hier vertretenen Auffassung bei der Beurteilung der Meldepflicht und der zu treffenden organisatorischen und technischen Massnahmen beizuziehen.

/8 Auch in diesem Bereich besteht ein Bedürfnis der Praxis, dass der **Bundesrat auf dem Verordnungsweg** die eine Meldepflicht begründenden Umstände, den Inhalt der zu erstattenden Meldung an den Beauftragten bzw. die betroffenen Personen sowie die möglichen organisatorischen und technischen Massnahmen zur Behebung der Verletzung des Datenschutzes bzw. zur Minderung ihrer möglichen nachteiligen Auswirkungen näher umschreibt. Der Bundesrat kann sich dabei an den Regelungen von Art. 33/34 DSGVO bzw. der Fachverbände für Informatiksicherheit orientieren.

/9 Nachdem die Erstattung einer Meldung weitgehend vom Ermessen des Verantwortlichen abhängt fehlt es an den rechtsstaatlichen Grundlagen für die Schaffung des Straftatbestandes von Art. 50 Abs. 2 Bst. e RevE DSG " Unterlassung der Meldung an den Beauftragten". Bestraft werden kann ein Verantwortlicher nach hier vertretener Auffassung höchstens, wenn er die Aufforderung des Beauftragten gemäss Art. 17 Abs. 2 RevE DSG zur Meldung einer Datenschutzverletzung an die betroffenen Personen vorsätzlich nicht befolgt.

Formulierungsvorschlag

**Art. 17** Meldung von Verletzungen des Datenschutzes

1 Der Verantwortliche meldet dem Beauftragen so rasch als möglich eine ihm bekannt gewordene unbefugte Datenbearbeitung oder den Verlust von Daten, wenn die Verletzung des Datenschutzes nach den Umständen voraussichtlich zu einem erhebliche Risiko für die Persönlichkeit und die Grundrechte einer grösseren Zahl von betroffenen Personen führt.

2 Der Verantwortliche informiert ausserdem die betroffenen Personen, wenn es zu ihrem Schutz erforderlich ist oder wenn der Beauftragte es aufgrund seiner Meldung ausdrücklich verlangt.

3 Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann der Verantwortliche die Meldung an die betroffenen Personen einschränken, aufschieben oder darauf verzichten.

4 Auftragsbearbeiter informieren den Verantwortlichen so rasch als möglich über eine ihnen bekannt gewordene unbefugte Datenbearbeitung oder einen Datenverlust.

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 Rat des von ihnen bezeichneten internen Datenschutzbeauftragten einzuholen und die getroffenen Massnahmen zu dokumentieren.

6 Der Bundesrat erlässt Bestimmungen über die Fälle in denen eine Datenschutz-Verletzung dem Beauftragten bzw. den betroffene Personen zu melden ist sowie über Inhalt und Struktur der Meldung und der Dokumentation der getroffenen Massnahmen im Falle einer Verletzung des Datenschutzes

**Art. 18 VE Rev DSG Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen**

/1 **"**Privacy by design" und "privacy by default" sind seit einigen Jahren "*Buzzwords*" in der Datenschutzdiskussion, obwohl bisher nicht ganz klar ist, mit welchen Mitteln und Verfahren diese Grundsätze in der Praxis umgesetzt werden sollen.

/2 Die gesetzlichen Vorschriften richten sich eigentlich in erster Linie an die Entwickler und Anbieter von Komponenten der IKT Infrastruktur, insbesondere der Software, obwohl diese in Art. 18 RevE DSG gar nicht erwähnt werden! Verantwortliche und Auftragsbearbeiter aber können zum Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen nur verpflichtet werden, wenn die entsprechenden Bearbeitungsmittel und Verfahren auf dem Markt zu angemessenen Bedingungen angeboten werden. In dieser Beziehung ist auf Art. 25 (1) DSGVO hinzuweisen, welche die Anwendung datenschutzfreundlicher Technik und Voreinstellungen in Zusammenhang mit den **Implementierungskosten** bringt.

/3 Abs. 2 ist die Verkörperung des Grundsatzes der "**Datenminimierung**" (Vgl. Art. 25 (1) DSGVO) und enthält ein **faktisches Verbot von "Big Data Analysen**, sofern diese zu personenbezogenen Ergebnissen führen. Dabei könnte durch "Big Data Analytics" in verschiedenen Bereichen, z.B. Diagnosesysteme bei E Health, oder Analyse von Hacking-Angriffen zu wertvollen und sehr erwünschten Ergebnissen führen. Sie sollten daher durch den Datenschutz nicht unnötig eingeschränkt oder behindert werden. Der Gesetzgeber sollte sich dieser Problematik stellen, indem BMöglichkeiten zu datenschutzkonformen "Big Data Analysen" aufgezeigt werden, z.B. in Anlehnung an die Bestimmungen zum "Profiling".

/4 Als ausgesprochen kritisch ist hingegen die **Übergangsbestimmung** von Art. 59 Bst. b RevE DSG zu beurteilen, welche die Verantwortlichen und die Auftragsbearbeiter verpflichtet innert zwei Jahren nach Inkrafttreten des Rev-DSG die bisher nur vom Grundgedanken und der allge-

meinen Zielsetzung her erfassbaren organisatorischen und technischen **Anpassungen für bestehende Anwendungen** zu realisieren. Die Umsetzung dieser Obliegenheit kann mit sehr hohen Aufwendungen verbunden sein, die zwar zur Förderung des Datenschutzes beitragen, die Anwender von datenbearbeitenden Systemen aber erheblich belasten. Und umso mehr stört, dass die Unterlassung der Umsetzung dieser sich auf Allgemeinplätze beschränkenden Grundsätze mit einer Busse von 250'000 bis CHF 500’00 bedroht ist.

/5 Auch in dieser Angelegenheit empfiehlt sich die Anwendung des bisher im Rahmen der Vernehmlassung zum RevE DSG entwickelten Konzeptes: (1) Der Beauftragte sollte - möglichst frühzeitig! – Empfehlungen zum Datenschutz durch Einsatz der im Markt zu angemessenen Bedingungen verfügbaren technischen Mittel (Hardware) und datenschutzfreundlichen Vorrichtungen (Software) herausgeben bzw. den Zugang zu solche Mitteln und Verfahren erleichtern; er sollte diese Empfehlungen den aktuellen Entwicklungen der Informatik anpassen; und (2) bei der Umsetzung der Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen ist der betriebliche Datenschutzbeauftragte beizuziehen.

Formulierungsvorschlag

**Art. 18** Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1 unverändert

2 unverändert

3 Der betriebliche Datenschutzbeauftragte ist bei der Umsetzung der organisatorischen und technischen Massnahmen zum Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen beratend beizuziehen.

4 Der Beauftragte erlässt Empfehlungen zu den Mitteln und Verfahren für den Datenschutz durch Technik und datenschutzfreundliche Vorstellungen und aktualisiert diese nach dem jeweiligen Stand der Technik

**Art. 20 DSGVO Stärkung der Rechte betroffener Personen: Recht auf Datenübertragbarkeit**

Nachstehend soll kritisch geprüft werden, inwieweit die im harmonierten europäischen datenschutzrecht neu eingeführten Rechte betroffener Personen deren Stellung gegenüber den Verantwortlichen und Auftragsbearbeitern tatschlich verbessern

/1 Das **Recht auf Datenübertragbarkeit** ("*Portabilität*" nach Art. 20 DSGVO) ist Ausdruck weniger des Datenschutzes als des Wettbewerbsrechts: Es geht auch bzw. vor allem um die **Verhinderung des Aufbaus einer marktbeherrschenden Position** der bearbeitenden Stellen gegenüber den betroffenen Personen. Im schweizerischen Recht ergibt sich die Pflicht zur Herausgabe anvertrauter Daten übrigens auch aus dem auf alle Arbeitsverhältnisse anwendbaren Art. 400 OR.

/2 Daneben müsste das Verhältnis der Datenherausgabe zu den **Aufbewahrungspflichten** beim Verantwortlichen und zum wohlverstandenen Recht auf **Sicherung von Beweisunterlagen** geklärt werden (Art. 958f OR und Geschäftsbücherverordnung SR 221.431 sowie zu den zahlreiche Aufbewahrungs- und Nachweispflichten im Wirtschaftsverwaltungsrecht). Denn der Datenschutz ist zeifellos Teil der Gesamtrechtsordnung unseres Landes und muss mit diesen Regelungen verträglich sein

**Das Recht auf Vergessen(werden)**

/1 Das sog. "**Recht auf Vergessen(werden)**" ist seit dem Urteil des EUGH vom 13.5.2014 in der Rechtssache C-131/12 Mario Costeja Gonz lez ein typisches und oft missverstandenes "*Buzzword*" in der Datenschutz-Szene. Das EUGH Urteil bezieht sich nämlich **n u r auf die Eintragungen in Suchmaschinen** wie Google. Ein allgemeines Recht auf Vergessen kann es schon aus Gründen der Einhaltung der Aufbewahrungspflichten, der Sicherstellung von Beweisunterlagen und der oft überwiegenden Interessen der bearbeitenden Stellen (Art. 13 Abs. 1 DSG) nicht geben.

/2 Im Übrigen ist das "Recht auf Vergessen" schon im geltenden Recht durch den Anspruch auf Sperrung oder Vernichtung ("Löschung") der Personendaten gewährleistet (Art. 28a Abs. 1 ZGB iVm Art. 15 Abs. 1 DSG).

/3 Bei der Forderung für ein "Recht auf Vergessen" muss nach hier vertretener Auffassung immer auch das wohlverstandene Interesse der Rechtsgemeinschaft beachtet werden, dass gewisse Informationen über eine betroffene Person (wie z.B. bestimmte Straftatbestände, Massnahmen, Insolvenz) erhalten bleiben und verfügbar sind. Es sollte somit vermieden werden, dass das "Recht auf Vergessen" für eine private Zensurierung der vor allem in sozialen Netzwerken vorhandenen und oft von den betroffenen Personen einmal selbst eingegebenen Datenbestände missbraucht wird.

/4 Wie der EDÖB in seiner Beurteilung des "Rechts auf Vergessen" zutreffend hingewiesen hat sollte es **vor allem Sorge der betroffenen Personen** sein, die Speicherung personenbezogener Informationen im Internet, v.a. in den sozialen Netzwerken, **eigenverantwortlich einzuschränken**.
https://www.edoeb.admin.ch/datenschutz/00683/01173/index.html?lang=de

**Umsetzung von Datenportabilität und des Rechts auf Vergessen**

/1 Die Umsetzung des Rechts auf Datenübertragbarkeit sowie des Rechts auf Vergessen könnte aufgrund der heutigen technischen und gesellschaftlichen Verhältnissen der Universalität und Ubiquität der elektronischen Bearbeitung von Personendaten *("ubiquitous computing*"), v.a. in den sozialen Netzwerken, zu unvorhergesehenen Folgen ("*unintended consequences*") führen, v.a. wenn diese Rechte auch die **riesigen Bestände von Archiv- und Sicherungsdaten** umfassen sollten.

/2 Denn wenn einzelne Datensätze in einer Archiv- oder Sicherungsdatei gelöscht werden müssten, könnte das sehr erhebliche Folgen für die weitere Nutzung der Daten und die Gewährleistung der Datensicherheit nach sich ziehen. Im Zweifel sollte daher die **Sperrung** der Daten gegen jede weitere Bearbeitung für die Zwecke des Datenschutzes genügen bzw. bewilligt werden.

**Mögliche verfahrensrechtliche Verstärkungen der Rechtstellung der betroffenen Personen**

/1 Zunächst ist zu prüfen, ein Bedarf besteht, das geltende schweizerische Recht dem europäischen Standard in Bezug auf die Durchsetzung von Ansprüche aus dem Datenschutz gegen Verantwortliche oder Auftragsbearbeiter dem harmonisierten europäischen Datenschutzrecht anzupassen. Eine kritische Würdigung der im geltenden schweizerischen Recht geltenden Normen zeigt dass wir die in Art. 79 DSGVO enthaltenen Regeln weitgehend erfüllen oder sogar übertreffen.

/2 Art. 15 DSG-1992/2006 enthält einen Verweis auf die Ansprüche aus Persönlichkeitsschutz nach Art. 28g-281 ZGB. Der Anspruch auf Schadenersatz ergibt sich aus Art. 28a Abs. 3 ZGB. Zusätzlich

entsteht bei Persönlichkeitsverletzung gemäss Art. 49 OR von Gesetzes wegen ein Anspruch auf Genugtuung.

/3 Im Hinblick auf die Erleichterung der Durchsetzung der Ansprüche betroffener Personen aus Persönlichkeitsverletzungen kann auf Art. 33 Abs.2 iVm Art. 129 IPRG verwiesen werden: Dadurch wird für Klagen aus Persönlichkeitsverletzungen die Zuständigkeit schweizerischer Gerichte am Handlungs- oder Erfolgsort begründet. Dies entspricht nach hier vertretener Auffassung auch der Regelung von Art. 5 (3) LugÜ. Für Klagen auf Durchsetzung gilt Art. 130 Abs. 3 IPRG in der Ergänzung gemäss Art. 130 Abs. 3 RevE DSG: Zuständigkeit schweizerischer Gerichte auch am Ort wo die betreffende Datensammlung geführt wird. Gemäss Art. 20 ZPO ist für Klagen aus der Verletzung des Datenschutzes auch die Zuständigkeit des Gerichts am Sitz der betroffenen Person gegeben. Im Vergleich zur Gerichtsstandsregelung von Art. 79 (2) DSGVO wäre daher allenfalls das schweizerische IPRG bei Ansprüchen aus dem Datenschutz um die Zuständigkeit der schweizerischen Gerichte am Aufenthaltsort der getroffenen Person zu ergänzen.

/4 Zur vefahrensrechtlichen Stärkung der Stellung betroffener Personen könnte in Analogie zu Art. 10 Abs. 2 Bst. b. UWG und in Anlehnung an Art. 89 ZPO ("Verbandsklage") ein Klagerecht von Organisationen geschaffen werden, welche sich statutengemäss dem Datenschutz widmen. Im Weiteren könnte, in Analogie zu Art 13a UWG und zur Beurteilung der Zulässigkeit einer Wettbewerbsbeschränkung nach Art. 15 KG an Beweiserleichterungen für die betroffenen personen gedacht ewerden: vgl. Prof. Hardy Landolt "Beweiserleichterungen und Beweislastumkehr im Arzthaftungsprozess"; Dr. Lucas David, "Beweislastumkehr bei Tatsachenbehauptungen in der Werbung" https://www.walderwyss.com/publications/335.pdf Dies würde bedeuten, dass nicht die betroffene Person eine Verletzung der Datenschutzvorschriften, sondern der Verantwortliche oder Auftragsbearbeiter deren Einhaltung nachzuweisen hat. In diesem Bereich besteht daher auch nach Auffassung des Unterzeichnenden ein gewisser Freiraum zur verfahrensrechtlichen Besserstellung der betroffenen Personen in Übereinstimmung mit vergleichbaren Institutionen im schweizerischen Wirtschaftsrecht.

/5 Auf eine gewisse **Verwandtschaft von UWG und Wettbewerbsrecht** (Missbrauch der Wettewerbsfreiheit) **mit dem Datenschutz** (Verhinderung des Missbrauchs der Informationsfreiheit) wurde schon vor 30 Jahren im Rahmen der Arbeitsgruppe zur Schaffung des DSG-92 hingewiesen. So wurde z.B. das Verfahren vor dem EDÖB mit seiner Kombination von Abklärungen und Empfehlungen dem Verfahren vor der damaligen Kartellkommission nachgebildet. Auch ist denkbar, dass das von einer (z.B. auf einer Webseite) publizierten "Datenschutzerklärung" abweichende Verhalten einer datenbearbeitenden Stelle als unlauterer Wettbewerb im Sinne von Art. 3 Abs. 1 Bst b UWG zivil- und strafrechtlich geahndet werden könnte. https://www.iitr.de/veroeffentlichungen-des-instituts-fuer-it-recht/282-der-datenschutz-als-marktverhaltensregel-im-wettbewerbsrecht.html

**Art. 40 ff RevE DSG Überlegungen zur Verstärkung der Stellung des Beauftragten**

/1 Im DSG-1992/2006 hat der Beauftragte den Datenschutz in der Praxis vor allem durch die (in der Praxis von Verantwortlichen und Auftragsbearbeitern gerne in Anspruch genommene) Beratung der Anwender gemäss Art. 28 DSG sowie durch Herausgabe von Empfehlungen (auch in Form von Merkblättern, Leitfäden, Checklist und Musterverträgen) gefördert. Diese Tätigkeit beruhte auf dem **Vertrauen**

betroffener Personen und bearbeitenden Stellen zum Beauftragten. Diese bisher als zentral erachtete Aufgabe der Beratung von Verantwortlichen und Auftragsbearbeitern in Fragen des Datenschutzes gemäss Art. 28 DSG ist neu diskret in der Aufzählung "Weiterer Aufgaben des Beauftragten" in Art. 49 Bst. a RevE DSG untergebracht um nicht zu sagen "versteckt" worden.

/2 Der bisherige Ansatz der Aufgaben und Kompetenzen des Beauftragten hat sich nach hier vertretener Auffassung bewährt. Dieses auf Vertrauen und Kooperation mit den datenbearbeitenden Stellen beruhende Konzept wird nach hier vertretener Auffassung allerdings durch folgende neue Kompetenzen und Pflichten des Beauftragten in Frage gestellt, ja eigentlich in sein Gegenteil verkehrt:

a. Die auf Art. 42 RevE DSG gestützte Kompetenz des Beauftragten zu erhebliche Eingriffen in den Betrieb der Verantwortlichen und Auftragsbearbeiter indem der Beauftragte von sich aus **vorsorgliche Massnahmen** anordnen (und dies gemäss Art. 44 Abs. 3 RevE DSG **ohne aufschiebende Wirkung**, was in der Praxis zum Zusammenbruch der heute von der Verfügbarkeit der Informatik abhängigen Tätigkeit eines Unternehmens führen kann).
b. Der Beauftragte kann nach Art. 43 RevE DSG neu **Verfügungen (**nach Art. 5 VwVG) **über Verwaltungsmassnahmen** erlassen.(und diese gemäss Art. 292 StGB mit einer Strafdrohung bei Nichtumsetzung versehen).
c. Dem Beauftragten wird nach Art. 45 RevE DSDG eine **heikle Pflicht zur Anzeige** bei der Feststellung möglicher Verstösse gegen den Datenschutz auferlegt .
d. Er kann gemäss Art. 49 Bst. d RevE DSG betroffenen Personen Auskunft (und Rat) über die Ausübung ihrer Rechte erteilen.

/3 Mit der Zuweisung dieser neuen Aufgaben und Kompetenzen an den Beauftragten ist nach hier vertretener Auffassung eine **wesentliche Änderung der Rolle des Beauftragten** als neutraler, sachkundiger, unabhängiger - und daher von den Anwendern in der Praxis geschätzter – Vermittler in Datenschutzangelegenheiten verbunden. Dies könnte zu einer erheblichen Zurückhaltung der Verantwortlichen und Auftragsbearbeiter bei künftigen Kontakten mit dem Beauftragten in Datenschutzfragen führen. Darüber hinaus ist aufgrund der Kompetenzen des Beauftragten zum Erlass von Verfügungen und Verwaltungsmassnahmen mit einer zunehmenden Zahl von Rechtsstreitigkeiten zu rechnen.

/4 Es ist daher nach hier vertretener Auffassung zweifelhaft, ob die Ausdehnung der Kompetenzen und die Veränderung der Rolle des Beauftragten in der Praxis zu einer Verbesserung des Standes des Datenschutzes in unserem Lande beiträgt, oder – als *"unintended consequence"* - nicht die Umsetzung des Datenschutzes in der Praxis behindert und als Ergebnis das Datenschutz-Dispositiv unsere Landes schwächt.

/5 Nach hier vertretener Auffassung lässt sich eine gewisse Aufstockung von Ressourcen des EDÖB aufgrund der "Digitalen Transformation" rechtfertigen, allerdings g e r a d e **n i c h t in Zusammenhang mit den administrativen Aufgaben** wie z.B. Wahrnehmung der Melde-, Informations-, Prüf- und Konsultationspflichten, der Entgegennahme dokumentierter Datenschutz-Folgenabschätzungen oder der Archivierung der Meldung von Datenschutz-Verletzungen [Die entsprechenden Pflichten erinnern den

Unterzeichnenden an die frühere Praxis der schwedischen Datenschutzbehörde, wonach gemäss dem "Datalagen" vom 11. 5 1973 (vgl. dazu http://www.forstmoser.ch/publications/articles/1978-grundfragen.pdf FN 161) sämtliche automatisierten Bearbeitungen von Personendaten der Aufsichtsbehörde zu melden und zu registrieren waren: Was dann mit diesen in einem grossen Warenlager abgelegten Meldungen weiter zu geschehen hatte war in jener Frühzeit des Datenschutzes niemandem so richtig klar ...].

/6 Im privatrechtlichen Bereich sollte nach hier vertretener Auffassung das Schwergewicht der künftigen Tätigkeit des Beauftragten und seines Stabes vor allem auf einen **Beitrag zur Entwicklung von "*good practices*" und Empfehlungen** gemäss Art. 8 RevE DSG gelegt werden, wobei solche Empfehlungen noch verstärkt durch Zusammenarbeit des Beauftragten und seines Stabes mit den Vertretern der bearbeitenden Stellen und den betroffenen Personen in spezifischen Bereichen zu erarbeiten sind.

Die Entwicklung einer solchen "**Datenschutz-Deontologie**" für spezifische Gebiete der Bearbeitung von Personendaten wurde schon vor 30 Jahren im Schoss der Arbeitsgruppe des Bundesrates für die Entwicklung des DSG diskutiert, hat im DSG-92 wegen der Neuheit der Institution aber keinen Niederschlag gefunden. Dagegen findet sich eine solche Möglichkeit in § 38a BDSG und hat dort die Entwicklung des "**Code-of-Conduct-Datenschutz**" durch den Gesamtverband der deutschen Versicherungswirtschaft bewirkt https://de.wikipedia.org/wiki/CoC-Datenschutz

Eine entsprechende Bestimmung wurde in Art. 27 Richtlinie 95/46 EG aufgenommen "Entwicklung von Verhaltensregeln zur Durchsetzung von Datenschutzvorschriften" http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE und hat insbesondere zur Einsetzung der **Europäischen Datenschutzgruppe** gemäss Art. 29-30 Richtlinie 95/46 / EG geführt, welche intensive und äusserst wertvolle Studien zur Umsetzung des Datenschutzes in verschiedenen durch die Entwicklung der Informationstechnologie beeinflussten Bereichen durchgeführt hat, in letzter Zeit z.B. zu den Herausforderungen von "Big Data" und dem Einsatz von "Drohnen" http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

/7 Zusammenfassend halten wir somit nicht die Aufstockung der Ressourcen des Beauftragten zur Wahrnehmung der im RevE DSG enthaltenen zahlreichen administrativen Kontroll-, Informations-, Melde-, Konsultations- und Prüfpflichten wohl aber die in Art. 8-9 RevE DSG vorgesehene Entwicklung von **Empfehlungen der guten Praxis** durch den Beauftragten in Zusammenarbeit mit den interessierten Kreisen (je nach den Umständen Verantwortliche, Auftragsbearbeiter und betroffene Personen) als eine der grundlegenden und praxisrelevanten Voraussetzungen für die sach- und zeitgerechte Entwicklung und Anpassungen des Datenschutzes im Zeitalter der "Digitalen Transformation der Informationsgesellschaft".

/8 Damit könnte in gewisser Weise wieder der Stand der Entwicklung der Grundsätze zum Datenschutz in den 80er Jahren des letzten Jahrhunderts erreicht werden, als in der vom Bundesrat eingesetzten Arbeitsgruppe nicht nur Professoren, Anwälte und Angehörige der öffentlich-rechtichen Datenschutz-Administration vertreten waren, sondern - nach persönlicher Erinnerung des Unterzeichnenden - namentlich Angehörige von Industrie, Informatik, Versicherungswirtschaft, des Bankenplatzes, der Marktforschung, des Gewerkschaftsbundes, führende Experten für Persönlichkeits-, Wirtschafts-, Immaterialgüter- und Arbeitsrecht, eine Stadtpräsidentin und Mitglied der Bundeversammlung, die bundesnahen Betriebe (Post; Telecom; SBB), das Bundesamt für Justiz, die Bundesanwaltschaft und der militärische Sicherheitsdienst, welche kollegial die Interessen der bearbeitenden Stellen und der betroffenen Personen wahrgenommen haben.

## Art. 41bis RevE DSG Gewährleistung der Geheimhaltung in Datenschutzverfahren

/1 Aus der Prüfung der im Rahmen der Revision des DSG geschaffenen neuen Rechtsinstitute hat sich ergeben, dass der Beauftragte in Zukunft über sehr viele Unterlagen und Informationen verfügen wird, welche der Geheimsphäre der bearbeitenden Stellen angehören und von den Verantwortlichen und Auftragsbearbeitern als vertraulich betrachtet werden werden und nach hier vertretener Auffassung als deren Geschäftsgeheimnisse qualifizieren.

/2 Nun untersteht der Beauftragte jedoch nach herrschender Lehre dem Öffentlichkeitsprinzip (Art. 2 Abs. Bst. a 1 BGÖ; vgl. David Rosenthal, in "Datenschutzrecht", § 7 Sanktionierung von Datenschutzverstössen, S. 219, Rz 7.42 FN 60). Das bedeutet, dass grundsätzlich jedermann gestützt auf das Öffentlichkeitsgesetz ("BGÖ") in die dem Beauftragten im Rahmen der erweiterten Kompetenzen des Beauftragten zur Durchführung einer Untersuchung (Art. 41 RevE DSG), einer Datenschutz-Folgenabschätzung nach Art. 16 RevE DSG, oder der Meldung einer Datenschutzverletzung nach Art. 17 RevE offenbarten internen Informationen bzw. gelieferten Unterlagen und Dokumentationen Einsicht nehmen und Zugang beanspruchen kann (Art. 6 Abs. 1 BGÖ).

/3 Dies erscheint besonders heikel in Fällen wo bei der Meldung einer Datenpanne nach Art. 17 RevE DSG Datenlecks offenbart und Schwachstellen der Datensicherheit nachgewiesen werden. Entsprechend könnten die beim Beauftragten vorhandenen Unterlagen aus Untersuchungen, Folgenabschätzung und Meldungen über Datenpannen eine Fundgruppe für potentielle Hacker und Täter eines Computerdelikts nach Art. 143, 143bis, 144bis, 147 StGB darstellen. Aber auch die Einsicht in eingereichten Unterlagen über eine Datenschutz-Folgenabschätzung könnten den Mitbewerbern einer bearbeitenden Stelle wichtige Aufschlüsse und Erkenntnisse bieten.

/4 Es ist zweifelhaft ob Art. 3 Abs. 1 Bst. a und Art. 7 BGÖ ausreichen, um die beim Beauftragten in Zukunft in erheblichem Umfange vorhandenen Unterlagen über Bearbeitungsvorgänge und interne Datenbestände vor dem Missbrauch des Öffentlichkeitsprinzips zu schützen (vgl. David Rosenthal, in "Datenschutzrecht", § 7 Sanktionierung von Datenschutzverstössen, S. 219, Rz 7.42 FN 61). Diesbezüglich ist darauf hinzuweisen, dass der Beauftragte aufgrund seiner Doppelrolle als Hüter des Datenschutzes wie auch als Verantwortlicher für die Umsetzung des Öffentlichkeitsprinzips in einen heiklen Interessenkonflikt geraten kann.

/5 Es ist nach hier vertretener Auffassung daher zu prüfen, ob für die dem Beauftragten offen gelegten Unterlagen und Informationen im Rahmen einer Untersuchung, einer Datenschutz-Folgenabschätzung bzw. einer Meldungen über Datenschutzverletzungen nicht ein angemessenes Schutzdispositiv für die bearbeitenden Stellen (Verantwortliche und Auftragsbearbeiter) geschaffen werden kann. Dabei könnte man sich wie schon bei der Entwicklung der Kompetenzen des Beauftragten bei der Schaffung des DSG-92 an den Regeln des Wettbewerbsrechts orientieren.

Formulierungsvorschlag (zur kritischen kritische Prüfung)

Art. 41bis Amts und Geschäftsgeheimnisse

1 Der oder die Beauftragte und das Sekretariat wahrt das Amtsgeheimnis für die ihm oder ihr von privaten Personen mi Rahmen seiner oder ihrer Tätigkeit zugänglich gemachten internen und vertraulichen Unterlagen und Informationen.

2 Er oder sie darf Kenntnisse, die sie bei ihrer Tätigkeit erlangen, nur zu dem mit der Auskunft oder dem Verfahren verfolgten Zweck verwerten.

3 Die Veröffentlichungen des oder der Beauftragten dürfen keine Geschäftsgeheimnisse preisgeben.

**Art. 50-51 revE DSG Strafbestimmungen**

/1 Grundlage für die Verfolgung von Datenschutz-Delikte könnte das Gesetz über das Verwaltungsstrafrecht (VStrR). Die für die Verfolgung der von Privatpersonen begangenen Datenschutzdelikte zuständige Behörde wäre u.E. nach den Grundsätzen des VStrR noch zu bestimmen.

/2 Es dürfte keine eingehendere Begründung erfordern, dass die Strafbestimmungen nach Art. 50-51 revE DSG dem elementaren strafrechtlichen Grundsatz der *"nulla poena sine lege scripta stricta praevia"* widersprechen, der in Europa aus der Aufklärung hervorgegangen, von Anselm von Feuerbach in seinem 1801 in Giessen herausgegebenen "Lehrbuch des gemeinen, in Deutschland geltenden peinlichen Rechts" formuliert wurde und verkürzt in Art 1 StGB seinen Niederschlag gefunden hat.

/3 Datenschutzregeln, welche den bearbeitenden Stellen ein erhebliches Ermessen bei der Beurteilung des Vorhandenseins Pflichten aus dem Datenschutz auferlegen, eignen sich aufgrund des die Strafverfolgung beherrschenden "Legalitätsprinzips" grundsätzlich nicht zur Aufstellung einer Strafnorm. Das trifft nach hier vertretener Auffassung für folgende Datenschutzvorschriften und der damit verbundenen Strafdrohung zu:

- Art. 5 Abs. 1 iVm Art. 51 Abs. 1 Bst. a RevE DSG Beurteilung des Risikos für die Persönlichkeit der betroffenen Personen bei einer Ausland-Bekanntgabe
- Art. 7 Abs. 1 und 2 iVm Art. 51 Abs. 1 Bst. b RevE DSG: Sorgfaltspflichten bei der Erteilung eines Auftrages für das Outsourcing der Datenbearbeitung
- Art. 11 iVm Art. 51 Abs. 1 Bst. c RevE DSG: Unterlassung angemessener technischer und organisatorischer Massnahmen zur Datensicherung
- Art. 13 und Art. 14 Abs. 2 Bst. b iVm Art. 50 Abs. 1 Bst. a und b RevE DSG: Strafdrohung trotz möglicher Freistellung von der Informationspflicht
- Art. 15 Abs. 1RevE DSG: Beurteilung der Auswirkung einer automatisierten Einzelentscheidung iVm der Strafdrohung nach Art. 50 Abs. 1 Bst. b RevE DSG
- Art. 16 Abs. 1 RevE DSG: Beurteilung des Vorhandenseins einer Pflicht zur Durchführung einer Datenschutz Folgenabschätzung iVM Art. 50 Abs. 1 Bst. c und Art. 51 Abs. 1 Bst. d RevE DSG
- Art. 17 Abs. 1 und Abs. 4 RevE DSG: Beurteilung der Voraussetzungen für die Meldung einer Datenschutz-Verletzung an den Beauftragten iVm Art. 50 Abs. 2 Bst. e und abs. 3 Bst. b RevE DSG
- Art. 18 iVm Art. 51 Abs. 1 Bst. e RevE DSG: Unterlassung der Anwendung datenschutzfreundlicher Vorkehrungen
- Art 19 Bst. b RevE DSG: Pflicht zur Informierung von Daten-Empfängern über Datenschutz-Verletzungen iVm Art. 50 Abs. 3 Bst. a RevE DSG

Die meisten vorstehenden Strafbestimmungen betreffen administrative Pflichten, insbesondere Meldungen an den Beauftragten. Inwieweit diese Meldungen überhaupt dem Datenschutz dienen, sei dahingestellt. Und der Datenschutz wird auch durch die Strafdrohung für die Vernachlässigung von Meldepflichten nicht gestärkt. Die in Art. 50/51 RevE DSG aufgeführten Tatbestände stimmen auch mit den Bussgeld-Vorschriften von Art. 83 DSGVO nicht überein!

/4 Darüber hinaus erscheint es nach wie vor störend, dass in einem Gesetz, welches sowohl für die Bearbeitung von Personendaten durch private Verantwortliche und Auftragsbearbeiter wie auch durch Angehörige der Bundesverwaltung gilt, nur privatrechtlich tätige bearbeitende **Stellen** mit Strafsanktionen bedroht werden. Es gibt ja in unserem Strafrecht eine ganze Reihe von Bestimmungen über sog. "Amtsdelikte" (Art. 312 ff StGB), und es ist nicht einzusehen, weshalb sich nur Private, nicht jedoch Amtspersonen einer kriminellen Verletzung von Datenschutzvorschriften schuldig machen können. Und weil Datenschutzverletzungen in der Regel durch ein arbeitsteiliges Zusammenwirken mehreren Personen begangen werden, drängt sich die Anwendung der Art. 6-7 VStrR auf.

/5 Die Strafbestimmungen nach Art. 50-51 RevE DSG sind daher in ihrer Gesamtheit als untauglich und nicht zielführend zu verwerfen. Es wäre anzustreben, eine Reihe von Tatbeständen zu entwickeln, welche strafwürdige Verletzungen des Schutzes der Persönlichkeit und der Grundrechte betroffener Personen beinhalten. Im Sinne einer vorläufigen gedanklichen Überlegung könnte man folgende Straftatbestände in Erwägung ziehen:

- Heimliche, gewaltsame, täuschende, betrügerische (z.B. Vorspiegelung eines Spiels oder Wettbewerbs) oder unter Drohung (mit Nachteilen) oder unter Duldung ausgeführte Beschaffung, Bearbeitung und Bekanntgabe von Daten nach dem uralten Grundsatz des römisches Rechts *"nec vi nec clam nec precario*"
- Schon heute mit Sanktion bedrohte ungültige Zustimmung zur Datenbearbeitung unter Verletzung von Art. 8 UWG (Verwendung missbräuchlicher Geschäftsbedingungen) bzw. Art. 7 KG (Unzulässige Verhaltensweisen marktbeherrschender Unternehmen, wie z.-B. Amazon oder Google!)
- Vorsätzliche Erteilung einer falschen oder unvollständigen Auskunft (wie heute Art. 34 Abs. 1 DSG)
- Vorsätzliche Erteilung falscher Auskünfte an den Beauftragten oder Verweigerung der Mitwirkung bei einer Überprüfung (Heute Art. 34 Aba. 2 Bst. b DSG)
- Verletzung der in einer "Datenschutzerklärung" (inbesondere einem "Website Privacy Statement") gemäss Art. 13 RevE enthaltenen Angaben über Art, Umfang und Zweck der Bearbeitung von Personendaten bzw. deren Bekanntgabe an Dritten
- Bekanntgabe von Personendaten ins Ausland trotz erkennbarer Gefährdung der Persönlichkeit der betroffenen Personen nach Art. 5 abs. 1 RevE DSG und ohne Datenschutzmassnahmen nach Art. 5 Abs. 3 RevE DSG

- Unterlassung der Durchführung und Dokumentation einer Datenschutzfolgeabschätzung nach Art. 16 bei der Bearbeitungen von Daten mit einem klar erkennbaren Risiko für die betroffenen Personen: Heikle Abgrenzung!
- Unterlassung von Massnahmen der Benachrichtigung der betroffenen Person sowie keine dokumentierte Massnahmen zur Minderung der Auswirkungen einer Datenschutzverletzung nach Art. 17 RevE DSG Ebenfalls heikle Abgrenzung
- Schon vorhanden in Art. 179novis StGB Unbefugtes Beschaffen von Personendaten
- Schon vorhanden: Verletzung der beruflichen Schweigepflicht nach Art. 35 DSG

Die vorstehende Liste dürfte die in Frage kommenden Straftatbestände bei datenschutzwidrigem Verhalten recht weitgehend umschreiben

Aarau, 4. April 2017

Beat Lehmann

## Amstutz Jonas BJ

**Von:** lars@luenenburger.ch
**Gesendet:** Dienstag, 4. April 2017 22:43
**An:** Amstutz Jonas BJ
**Betreff:** Stellungnahme zur Vernehmlassung Bundesgesetz über die Totalrevision des Datenschutzgesetzes
**Anlagen:** Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de_lue.doc

Sehr geehrter Herr Amstutz

Angehängt sende ich Ihnen meine Stellungnahme zur Vernehmlassung über den «**Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz**»

Mit freundlichen Grüssen
Lars Lünenburger

Gesendet von Mail für Windows 10

**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. Lars Lünenburger

Abkürzung der Firma / Organisation : lue

Adresse : Bahnhofstrasse 33a

Kontaktperson : Dr. Lars Lünenburger

Telefon : 044 362 13 61

E-Mail : lars@luenenburger.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

## Allgemeine Bemerkungen

| Name/Firma | Bemerkung/Anregung |
|---|---|
| lue | Das Schweizerische Datenschutzgesetz sollte mit der Europäischen Datenschutzgrundverordnung soweit kompatibel sein, dass die wirtschaftliche Zusammenarbeit nicht durch datenschutzrechtliche Grenzbarrieren unnötig behindert wird. Dies soll nicht durch die unreflektierte Übernahme der Datenschutzgrundverordnung geschehen. Sie kann aber insofern als Vorlage dienen, wie sie Veränderungen, Erkenntnisse und Lernen im Bezug auf das Europäische Rechtssystem zeigt.<br><br>Konkret definiert die Datenschutzgrundverordnung den Begriff Pseudonymisierung und erläutert das Kriterium identifizierbar (entspr. bestimmbar im DSG). Diese Definitionen sind in der heutigen Zeit wichtig, da mit der weitgehenden Digitalisierung der Welt, im Prinzip jede Einheit elektronischer Information einer Person, nämlich zumindest Ihrem Urheber, zugeordnet werden kann. Die Verwendung des nicht eingeschränkten Bestimmbar könnte damit alle Informationen unter den Datenschutz fallen lassen. Dies wäre nicht wünschenswert. Entsprechende Definitionen im Gesetz – und nicht nur in dem Erläuternden Bericht – sind wichtig und notwendig. |
| lue | Konkretes, aber hypothetisches Beispiel: Für eine Gesundheitsstatistik können Ärzte auf einer Webseite das Auftreten von Schnupfen durch Anklicken eines Buttons «Schnupfenfall aufgetreten» eintragen. Klickt ein Arzt z.B. am 03.04.2017 um 09:34 diesen Button, erscheint dies zunächst anonym, da der Patient/die Patientin nicht bestimmt werden kann. Legt man «bestimmbar» weit aus – so wie die jetzige Vorlage es definiert – kann der Patient aber mit nur 2 Datenquellen identifiziert werden: (1) IP-Adresse, von wo der Buttonklick kam, identifiziert den Arzt und (2) Behandlungskalender des Arztes identifiziert den Patient. Das erste bezieht sich v.a. auf die Identifizierung des Arztes, der dieser problemlos zustimmen könnte. Die zweite wäre aber für einen Aussenstehenden nur durch Verletzung von gesetzlichen Vorschriften (Schweigepflicht/Weitergabe durch den Arzt, Einbruch in den Computer des Arztes) zu erlangen. Die Hürde bei der Beschaffung der 2. Datenquelle sollte in der gesetzlichen Definition berücksichtigt werden.<br><br>(Ein öffentliches Interesse an der Verhinderung von Schnupfenepidemien sei für dieses Beispiel nicht berücksichtigt.) |
| lue | |
| lue | |
| lue | |

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

| Name/Firma | Gesetz | Art. | Abs. | Bst. | Bemerkung/Anregung |
|---|---|---|---|---|---|
| lue | DSG | 3 | 1 | j (neu) | Der Begriff Pseudonymisierung sollte eingeführt werden und in Anlehnung an die Europäische Datenschutzgrundverordnung definiert werden:<br>„Pseudonymisierung“: Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer bestimmten oder bestimmbaren natürlichen Person zugewiesen werden |
| lue | DSG | 3 | 1 | a. | Das in der Definition verwendete «bestimmbar» sollte genauer definiert werden. Diese Definition sollte sich an die Europäische Datenschutzgrundverordnung anlehnen:<br>Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; als bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann; |
| lue | DSG | 24 | 2 | e. 1. | Anonymisierung sollte hier oder in Artikel 3 definiert werden. Alternativ könnte Pseudonymisierung wie oben vorgeschlagen definiert werden. |
| lue | DSG | 31 | 2 | a. | dito |
| lue | DSG | 32 | 1 | a. | dito |
| lue | | | | | |

## 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 |
|---|---|
| lue | - |
| lue | |
| lue | |

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

| Name/Firma | Bemerkung/Anregung |
|---|---|
| lue | - |
| lue | |
| lue | |

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

| Name/Firma | Kapitel-Nr. | Bemerkung/Anregung |
|---|---|---|
| lue | | - |
| lue | | |
| lue | | |

## Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

| Name/Firma | Art. | Bemerkung/Anregung |
|---|---|---|
| lue | | - |
| lue | | |
| lue | | |

## Amstutz Jonas BJ

**Von:** Sylvain Métille <metille@hdclegal.ch>
**Gesendet:** Montag, 20. März 2017 15:11
**An:** Amstutz Jonas BJ
**Betreff:** consultation LPD
**Anlagen:** Revision_LPD_ sme.doc; Plaidoyer 2-17.pdf

Cher Monsieur,

Vous trouverez en annexe mes observations sur l'avant-projet de révision de la LPD. Je suis à disposition en cas de questions.

Bien à vous,

Sylvain MÉTILLE
Dr, avocat, chargé de cours à l'Université

*Leading lawyer in TMT (Chambers Europe 2015/2016, Legal500 EMEA 2014/2015)*

**HDC | Étude d'avocats | Law Firm**
Avenue Auguste Tissot 2bis
CP 851
CH - 1001 Lausanne
T 021 310 73 10
F 021 310 73 11
@smetille
www.hdclegal.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 : Sylvain Métille, Dr en droit, avocat, chargé de cours à l'Université

Abréviation de la société / de l'organisation : SME

Adresse : Av. Auguste-Tissot 2bis, 1006 Lausanne

Personne de référence :

Téléphone : +41 21 310 73 10

Courriel : metille@hdclegal.ch


Date : 20.03.2017

**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

**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 : |
|---|---|
| SME | Le 11 septembre 2014, le Conseil de l'Union européenne a adopté le rapport du comité d'évaluation concernant la protection des données en Suisse qui contient une recommandation qui invite la Suisse à renforcer les pouvoirs du préposé en lui attribuant des pouvoirs décisionnels et de sanctions. C'est également la tendance dans les autres pays. Malheureusment l'avant-projet ne renforce pas réellement les pouvoirs du PFPDT. Ce point doit être corrigé et de vrais pouvoirs de sanction (procédure administrative) doivent être donnés au PFPDT. Le recours à des sanctions pénales ne fonctionne pas et il faut donner au PFPDT les moyens correspondant à sa mission. La protection des données est une notion de droit civil. Ce n'est pas à une personne d'en assurer le respect. |
| SME | La révision de la LPD doit aussi prendre en compte les évolutions européennes, en particulier le projet de Règlement européen vie privée et communications qui entrera en vigueur également le 25 mai 2018. |
| SME | En anglais, l'abréviation DPA est habituellement utilisée pour Data Protection Autorithy. Il serait préférable d'utiliser FADP pour Federal Act on Data Protection. |
| SME | La loi devrait prévoir l'obligation pour les responsables du traitement étrangers qui collectent des données en Suisse, visent les résidents suisses ou utilisent des moyens de traitement en Suisse d'avoir un représentant en Suisse comme le prévoit le RGPD. Sans cela le PFPDT va renoncer à toute action contre ces sociétés. |
| SME | L'avant projet n'aborde pas la question des drones. La loi sur les aéronefs doit être complétée pour obliger le respect des principes de protection des données par défaut et dès la conception comme obligation des constructeurs, voire rappeler le respect de la LPD pour l'utilisateur (y compris cas échéant comme condition d'autorisation). |

**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**

| | |
|---|---|
| SME | Le PFPDT doit pouvoir prononcer des amendes et celles-ci doivent viser les entreprises. Le recours à la procédure pénale est inutilement compliqué pour les responsables du traitement comme les personnes dont les données sont traitées. Il y a aussi une perte de contrôle du PFPDT sur la procédure et un risque de décisions contradictoires entre les procédures civiles, pénales et administratives. (S. Métille et D. Raedler, Révision de la LPD, des sanctions à contre-courant et à contre-raison, Plaidoyer 2/17, pp 38-43) Finalement, le recours à la procédure pénale conduit à un report de charges sur les cantons, qui n'accorderont pas les ressources nécessaires et la violation de la LPD ne sera pas sanctionnée. La Suisse deviendra un paradis pour les entreprises qui ne veulent pas respecter les principes de base. |
| SME | L'entrée en vigueur rapide de la loi est requise pour assurer la conformité avec la Directive. Il faut aussi éviter que les entreprises suisses et étrangères se mettent en conformité au niveau européen (Règlement) puis doivent à nouveau, une année plus tard, remettre en cause tout le traitement de leurs données pour prendre en compte quelques obligations supplémentaires du droit suisse. Cela pourrait pousser des entreprises soit à renoncer à la prise en compte du droit suisse, soit même à quitter la Suisse. L'impact de la date d'entrée en vigueur ne doit pas être sous-estimée et tout doit être mis en œuvre pour que la LPD révisée soit approuvée courant 2018. Le projet de loi et le message devront aussi être publiés très rapidement pour permettre aux responsables du traitement d'envisager les changements et la coordination internationale. |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |

**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**

## 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 : |
|---|---|---|---|---|---|
| SME | LPD | 2 | | | Le Tribunal fédéral a retenu, en vertu de la théorie des effets, que les images prises en Suisse et publiées d'une façon qui permet d'y accéder en Suisse également ont un lien prépondérant avec la Suisse, même si les images sont traitées à l'étranger et ne sont pas mises en ligne directement depuis la Suisse (ATF 138 II 346, cons. 3.3). La LPD doit néanmoins définir son champ d'application territorial comme le fait le RGDP. Cela permet au responsable de traitement de savoir à quelles obligations il est soumis. Cela assure aussi une meilleure sécurité du droit. Doivent ainsi être couverts les traitements de données effectués en Suisse ou depuis la Suisse (le responsable du traitement est basé en Suisse ou les moyens utilisés sont en Suisse), les données traitées sont celles de résidents Suisse. Dans ces hypothèses, le responsable du traitement doit avoir un représentant en Suisse auprès de qui la personne concernée peut faire valoir ses droits et qui peut recevoir valablement les communications du PFPDT. |
| SME | LPD | 2 | 2 | c | Si la LPD ne s'applique plus aux traitements des données par les autorités judiciaires, également lorsque les procédures ne sont plus pendantes, des normes supplémentaires doivent être prévues dans le CPP et le CPC. Le CPP ne traite par exemple que des procédures pendantes (art. 101 CPP). Les droits de la personne dont les données sont traitées sans qu'elle ne soit partie à la procédure ne sont pas non plus pris en compte. Le droit de consulter le dossier est réservé aux parties (art. 53 CPC). |
| SME | LPD | 2 | 3 | | La compétence de Surveillance des tribunaux devrait être données au PFPDT jusqu'à ce qu'une autorité indépendante soit prévue par la loi et en fonction. |
| SME | LPD | 3 | | f | Les données non personnelles ne doivent pas être incluses. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 5 | 2 | | L'art. 5 al. 2 devrait être complété pour préciser que dans un tel cas il ne peut pas être tenu responsable en cas d'atteinte à la personnalité, même si un tribunal devait remettre en cause le choix du Conseil fédéral. Idem si des contrats sont approuvés par le PFPDT. |
| SME | LPD | 5 | 2 et 3 | | La compétence de vérifier si un pays tiers est sûr devrait revenir au PFPDT au lieu du Conseil fédéral. L'exception de l'al. 3 lit a devrait être supprimée car ces pays doivent être ajoutés automatiquement à la liste de l'al. 2.<br>L'avant-projet ne distingue pas dans quels cas il s'agit d'une communication exceptionnelle au sens de l'art. 6 et il n'est pas possible de savoir si une communication basée sur le consentement peut avoir lieu de manière régulière. Est-ce-que l'acceptation de conditions générales d'un service fournit via Internet est toujours valable, cas échéant seulement pour une communication exceptionnelle ou aussi pour une communication ordinaire? |
| SME | LPD | 6 | 2 | | L'art. 6 al. 2 va engendrer un nombre important de notifications que le PFPDT aura peine à gérer. On peut se demander si elles sont vraiment utiles. |
| SME | LPD | 7 | 1 | b | Une obligation légale de garder le secret ne doit pas interdire la sous-traitance. Pourtant, la portée de l'art. 320 CP est largement contestée en doctrine. La norme semble interdire toute délégation de traitement, alors que cela est donc justifié par la Sozialadäquanz. L'introduction du récent art. 26a OIAF permet à des fournisseurs externes de prestations informatiques d'avoir accès à des données de l'administration qui ne sont pas accessibles au public et qui sont donc couvertes par le secret de fonction, ce qui semble contraire à l'art. 320 CP. La portée du secret de fonction doit être clarifiée dans le Code pénal parallèlement à la révision de la LPD et les conditions de l'outsourcing à l'étranger pour les données de l'administration clairement redéfinies. La sécurité du droit ne permet pas d'avoir un art. 26a OIAF qui permet la délégation de traitement, un art. 320 CP inadapté au monde numérique actuel et la LPD qui renvoie à d'autres normes. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 8 | | | La publication de recommandations très concrètes par le PFDPT est un élément positif. En revanche, le fait qu'il s'agisse de bonnes pratiques non contraignantes est problématique car les responsables de traitement ne sauront pas s'il s'agit d'un objectif idéal (bonnes pratiques allant au-delà de la loi), ou simplement du minimum légal à atteindre (art. 8). |
| SME | LPD | 9 | | | L'art. 9 est inutile car les recommandations de bonnes pratiques n'ont pas de force obligatoire. Il doit donc être supprimé. |
| SME | LPD | 11 | 2 | | La sécurité des données est un élément difficile à mettre en place pour un responsable de traitement. Il est important que le Conseil fédéral et le PFPDT donnent des critères précis et des recommandations techniques, et non seulement des principes généraux comme actuellement (art. 11 al. 2). |
| SME | LPD | 12 | | | Il est important de régler la question de la mort numérique et de l'accès aux données des personnes décédées (art. 12). Il n'est en revanche pas justifié d'utiliser des catégories différentes aux alinéas 2 (proches) et 4 (héritiers). L'al. 3 doit être reformulé pour préciser que le secret n'est pas opposable à celui qui demande l'accès si le secret était dans l'intérêt du défunt. Les deux conditions de l'al. 1 sont cumulatives car le défunt doit pouvoir refuser l'accès sans avoir à bénéficier en plus d'un intérêt prépondérant. |
| SME | LPD | 13 | 4 | | Si l'on peut saluer l'obligation d'avoir l'accord du responsable de traitement pour sous-déléguer un traitement, l'information de la personne concernée doit être plus limitée (art. 13 al. 4). Il n'est pratiquement pas envisageable de communiquer la liste de l'identité et les coordonnées de tous les sous-traitants, ainsi que les données ou catégories de données concernées. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 13 | 4 | | Si l'on peut attendre du responsable du traitement qu'il informe de l'existence de sous-traitants et communique sur demande l'identité de ces derniers, il ne parait en pratique pas envisageable que le responsable du traitement doivent informer toutes les personnes dont les données sont traitées à chaque fois qu'il y a un changement de sous-traitant. Cela est d'autant plus vrai que nombre de sous-traitants n'auront un accès que limité voire incident aux données. L'exigence d'information doit être réduite pour être pratiquable. |
| SME | LPD | 14 | | | Le commentaire de l'art. 14 semble indiquer qu'une information n'est pas nécessaire lorsque la personne a rendu les données accessibles. Cela devrait être précisé dans la loi, y compris s'il s'agit des données rendues publiquement accessibles ou communiquées au responsable de traitement. |
| SME | LPD | 16 | | | Aucune méthodologie n'est imposée pour l'analyse d'impact préalable (art. 16). Les principes de base doivent être précisés dans la loi, sinon il y a un risque que le PFPDT refuse une méthode ou en impose une autre sans base légale. Si l'intention est au contraire que le PFDPT établisse une procédure, la loi devrait le prévoir.<br><br>Le risque accru exigeant une analyse d'impact préalable doit être précisé. Le commentaire retient un risque accru si une utilisation abusive des données pourrait porter atteinte à la personnalité, à la dignité ou au bien-être de la personne. C'est pourtant le cas de presque la totalité des utilisations abusives de données, ce qui revient à généraliser l'analyse préalable. Cela n'est pas souhaitable.<br><br>L'analyse d'impact ne doit concerner que le responsable de traitement et pas le sous-traitant.<br><br>L'analyse d'impact va demander un travail important aux responsables de traitement. Il conviendrait donc d'aller au bout du processus et donner plus de poids à l'avis du PFPDT. Si le PFPDT donne son accord ou ne s'exprime pas dans le délai de trois mois des communications du résultat de l'analyse, le responsable de traitement doit pouvoir partir du principe que le traitement décrit est conforme et qu'il ne peut pas faire ensuite l'objet d'une procédure ou de sanction pour ce traitement.<br><br>Les objections du PFPDT ne jouent pas grand rôle non plus, puisqu'il n'y a pas de sanction. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 17 | | | La notion de perte de données utilisée à l'art. 17 n'est pas satisfaisante et peut être comprise comme une suppression des données. Or elle doit couvrir toutes les pertes de maîtrise sur les données, y compris les potentiels accès et copies. Le risque est d'ailleurs plus grand si les données sont copiées et pas simplement supprimées puisqu'elles peuvent être utilisées sans droit par des tiers. |
| SME | LPD | 17 | 1 | | Selon le texte du l'avant-projet, le responsable du traitement doit notifier sans délai au préposé tout traitement non autorisé, le non-respect de cette obligation étant une infraction pénale. Or, rédigé ainsi, le responsable du traitement devrait aussi notifier tout traitement non autorisé qu'il a lui-même effectué par exemple une utilisation de données dans un but autre que celui annoncé. Cela peut violer le droit de ne pas s'auto-incrimnier. De plus, le responsable du traitement devrait choisir entre respecter cette disposition et être sanctionné pour avoir violé la LPD, ou ne rien dire pour éviter d'être sactionné. Le texte devrait être modifié pour adresser les failles de sécurités et traitements non-autorisés de tiers.<br><br>Il ne faut pas non plus que la sanction risquée en cas d'annonce soit aussi lourde que l'absence d'annonce, sinon le responsable de traitement n'aura aucun intérêt de procéder à une annonce. |
| SME | LPD | 18 | | | Le respect des principes de protection des données par défaut et dès la conception ne doit pas seulement être une obligation du responsable de traitement dans son organisation, ce doit être aussi une obligation des constructeurs, fabriquants, développeurs. Si l'on pense à un logiciel informatique, à une caméra, un téléphone portable ou une voiture connectée, ce n'est pas le responsable du traitement (qui sera souvent l'utilisateur) qui pourra respecter ces principes mais c'est le fabriquant qui doit les appliquer et permettre leur application dès la conception/fabrication. |
| SME | LPD | 18 | | | La protection des données dès la conception n'est pas suffisante et une interdiction claire doit être faite aux fabriquants et développeurs de prévoir des portes dérobées (backdoors) et toutes autres mesures permettant un accès aux données à l'insu de la personne concernée. Si les entreprises suisses peuvent se prévaloir d'une telle garantie, elles auront un avantage très compétitif au niveau international. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 19 | | | Le devoir de documentation de tous les processus de traitement (art. 19) est une mesure qui peut être lourde pour les responsables de traitement et il est important qu'elle soit détaillée dans la loi. Si une ordonnance peut préciser certaines modalités, les éléments principaux doivent déjà être décrits dans la LPD.<br><br>La communication de la durée de conservation dans le cadre du droit d'accès est illusoire, car elle n'est souvent pas définie en pratique. Il convient d'y renoncer. Quant à l'al. 3, il devrait être supprimé et au besoin intégré à l'art. 15 pour une meilleure coordination. Le secret d'affaire du responsable de traitement va souvent s'opposer à la communication des critères retenus. La simple mention des données traitées peut déjà lui poser des difficultés. |
| SME | LPD | 19 | | | La section 4 ne traite que du droit d'accès, elle devrait donc s'appeler droit d'accès plutôt que droits de la personne concernée. |
| SME | LPD | 22 | | | L'art. 22 prévoit des exceptions au droit d'accès en faveur des médias. Une mention des autres secrets (par exemple le secret professionnel) serait judicieuse. |
| SME | LPD | 23 | 2 | | L'art. 23 al. 2 prévoit des cas d'atteinte à la personnalité. La lit. b. vise les traitements contre la manifestation expresse de la volonté de la personne concernée, la lit. d le profilage sans le consentement exprès de la personne concernée, alors que la lit. c concerne la communication à des tiers de données sensibles (indépendamment du consentement). La lit. c devrait seulement viser les cas où la communication a lieu sans consentement. |
| SME | LPD | 31 | | | L'art. 31 prévoit que les organes fédéraux proposent aux Archives fédérales de reprendre toutes les données personnelles dont ils n'ont plus besoin en permanence. Il ne tient pas compte des organes qui doivent archiver eux-mêmes leurs données conformément à l'art. 4 al. 3 LAr et l'annexe 2 OLAr. Ces dispositions doivent être coordonnées. |
| SME | LDP | 34 | 4 | | L'art. 34 al. 4 doit aussi être applicable aux privés. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 37 | | | Si le PFPDT dispose de son propre budget (art. 37), rien ne le lui garantit et le parlement pourrait le réduire drastiquement par mesure de rétorsion. L'indépendance de ses locaux et de son personnel n'est pas non plus garantie par la loi. On ne peut pas réellement parler d'un renforcement de son indépendance. |
| SME | LPD | 37 | 1 | | Pour assurer l'indépendance du PFPDT, il doit être élu par le Parlement. Le projet prévoit seulement une ratification du choix fait par le Conseil fédéral, ce qui laisse la possibilité au Conseil fédéral de sanctionner un préposé sortant et ne laisse pas de réel choix à l'assemblée. |
| SME | LPD | 40 | 3 | | Aucun arbitrage n'est prévu en cas de désaccord entre autorités au sens de l'art. 40 al. 3. Une compétence devrait être donnée, par exemple au TAF similaire à la cour des plaintes selon le CPP. |
| SME | LPD | 41 | | | L'art. 41 prévoit que le PFPDT peut requérir des renseignements et des documents. En cas de non coopération, le PFPDT peut inspecter des locaux et exiger l'accès à des documents. Le renvoi à l'art. 17 PA indique également que des témoins peuvent être entendus, mais l'art. 14 PA doit encore être complété. L'art. 44 renvoie également à la PA. Il conviendrait donc de préciser les moyens d'enquête du PFPDT et d'adapter la terminologie avec l'art. 12 PA (documents, renseignements des parties, renseignements ou témoignages de tiers, visite des lieux, expertises). La participation de l'organe fédéral ou de la personne privée visée aux mesures d'enquête et son droit d'être entendu doivent être garantis. |
| SME | LPD | 41 | | | Selon le commentaire, les mesures provisoires semblent également viser l'administration des preuves, alors que ces dernières sont traitées à l'art. 41. Il y a dès lors un risque que de moyens envisagés dans les mesures provisoires pour l'obtention des preuves ne soient pas reconnus. |
| SME | LPD | 41 | 3 | | Aucun moyen de contrainte n'est donné au PFPDT. La possibilité doit lui être donnée de demander l'assistance de la police fédérale ou cantonale pour mener des perquisitions si la personne ou l'organe visé refuse de coopérer. Les moyens de l'art. 41 al. 3 ne doivent pas être limités aux cas où la personne visée ne coopère pas, sinon il serait facile de faire disparaître des preuves. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 41 | 5 | | Le dénonciateur sera informé de l'issue de la procédure mais n'a pas qualité de partie. Cela n'est pas satisfaisant et une possibilité d'être partie devrait lui être donnée lors que ses données sont concernées. Sinon il devra ouvrir une procédure civile parallèle. Il y aurait ainsi une procédure civile et une procédure administrative portant sur le même objet et avec les mêmes buts, ce qui va doubler les efforts nécessaires pour arriver au même but. En l'absence de procédure collective, un responsable de traitement pourra devoir faire front à une procédure devant le PFPDT et une série de procédures civiles ouvertes devant différentes autorités pour le même traitement. Cela va engendrer de coûts inutiles et représente surtout un risque de décisions contradictoires. |
| SME | LPD | 42 | | | Les mesures provisoires de l'art. 42 permettent de préserver des preuves. Il s'agit toutefois seulement d'une mesure temporaire. La possibilité, au fond, d'administrer le moyen de preuve doit être prévue par la loi. Sinon il n'y a aucune raison de préserver provisoirement des preuves qui au final ne peuvent pas être utilisées. |
| SME | LPD | 48 | | | L'information du public doit être prévue dans la loi, et non seulement une information au dénonciateur. Toutes les décisions doivent être rendues accessibles car il s'agit d'une source de jurisprudence importante. L'art. 48 restreint actuellement trop les possibilités d'information. |
| SME | LPD | 49 | | | Le PFDPT doit aussi avoir la possibilité d'élaborer des outils, notamment informatiques, s'ils sont dans l'intérêt du public. On peut penser ainsi à certains outils par exemple proposés ou recommandés par la CNIL. Sans disposition ad hoc dans la loi, il pourrait être reproché au PFPDT, s'il développe un logiciel open source mis gratuitement à disposition des personnes intéressées, d'avoir une activité qui n'est pas prévue par la loi et de créer une distortion de concurrence. Il y a pourtant beaucoup de situations où les solutions commerciales ne prennent pas suffisamment en compte la protection des données. |

| | | | | | |
|---|---|---|---|---|---|
| SME | LPD | 50 | | | Le commentaire de l'art. 51 indique que cette disposition ne s'applique pas aux organes fédéraux, ce qui ne figure pas clairement dans le texte de la loi. Ce devrait aussi être le cas pour l'article 50. On peut en effet se demander si la notion de personne privée est à opposer à organe fédéral ou si elle fait référence à la personne individuelle au sein d'une entreprise ou organe fédéral. La personne privée pourrait donc être un fonctionnaire. Cela devrait être précisé, même si à notre sens seule la société, éventuellement l'organe fédéral, devrait être punissable. |
| SME | LPD | 51 | | | Le commentaire de l'art. 51 indique que cette disposition ne s'applique pas aux organes fédéraux, ce qui ne figure pas clairement dans le texte de la loi. On peut en effet se demander si la notion de personne privée est à opposer à organe fédéral ou si elle fait référence à la personne individuelle au sein d'une entreprise ou organe fédéral. La personne privée pourrait donc être un fonctionnaire. Cela devrait être précisé, même si à notre sens seule la société, éventuellement l'organe fédéral, devrait être punissable. La violation de la LPD n'est généralement pas un choix individuel, mais un choix, et donc une responsabilité, de la société et il n'y a, à priori, pas de raison de condamner pénalement l'employé d'une société et pas un fonctionnaire. |
| SME | LPD | 52 | | | A lire le commentaire, il faudrait préciser que les lettres de l'art. 52 sont alternatives et non cumulatives. Il est de plus fondamental de préciser que cet article ne concerne pas la révélation à un sous-traitant. |
| SME | LPD | 56 | | | Le RGPD prévoit que des amendes peuvent être infligées également à des entitées étrangères. Ainsi une autorité d'un Etat Membre pourrait infliger une amende à une société suisse, sans que cette dernière n'ait participé à la procédure. Il faut préciser que les traités internationaux visés à l'art. 56 ne peuvent pas servir à faire exécuter en Suisse une sanction prononcée à l'étranger. |

**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**

| | | | | | |
|---|---|---|---|---|---|
| SME | CP | 179 novies | | | Cet ajout est le bienvenu. L'art. 179novies prévoit dans sa nouvelle version que celui qui aura soustrait des données personnelles qui ne sont pas accessibles à tout un chacun sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. La notion « qui ne sont pas accessibles à tout un chacun » devrait être remplacée par celle de l'art. 143 CP (soustraction de données) à savoir « qui ne lui étaient pas destinées ». |
| SME | CO | 328b | | | La portée de l'art. 328b CO et du renvoi à la LPD divise la doctrine. La révision de la LPD doit aussi traiter de cette question et modifier au besoin l'art. 328b CO, afin qu'il ne soit pas plus limitatif. |
| SME | LJAr | 3 | | a | Le projet de loi sur les jeux d'argent définit les jeux d'argent comme les jeux qui, moyennant une mise d'argent ou la conclusion d'un acte juridique, laissent espérer un gain pécuniaire ou un autre avantage appréciable en argent. L'actuel art. 1 al. 2 de la loi sur les loteries et les paris professionnels contient une définition similaire. Le "paiement" en données personnelles n'est pas considéré comme une mise. Cette disposition doit être complétée de sorte que la mise à disposition obligatoire de données personnelles utilisables dans un autre but que la communication du gain, laissant espérer une chance de gain pécuniaire, doit être considéré de la même manière qu'une mise en argent. |
| SME | LPD | 25 | | | Le projet ne prévoit pas d'actions en exécution du droit d'accès (mentionnées pourtant à l'art. 15 al. 4 de la LPD actuelle). Il faudrait l'ajouter à l'art. 20 ou 25.<br><br>Alors que l'on pourrait imaginer qu'une action puisse, indirectement, se fonder sur les droits de la personne concernée issue de la protection de sa personnalité (et donc sur la voie de l'art. 25), le rapport explicatif semble faire une distinction entre l'action en exécution du droit d'accès et, justement, les actions de l'art. 25 à lire le commentaire en p. 86 du rapport (§ 8.2.9.1 relatif au for), qui est d'ailleurs le seul endroit du rapport mentionnant l'existence d'une action en exécution du droit d'accès. |
| SME | LPD | 12 | | | Le projet ne prévoit pas d'actions en exécution du droit à la consultation des données d'une personne décédée. Il faudrait l'ajouter à l'art. 12 ou 25. |
| SME | LPD | 20 | | | L'absence de réponse doit aussi être sanctionné pénalement (pas seulement la réponse incomplète). |

| | | | | | |
|---|---|---|---|---|---|
| SME | LTC | 45c | | | L'art. 45c LTC est la seule disposition applicable aux cookies. Elle doit être intégrée dans la révision de la LPD. Une lecture stricte exigerait une information pour chaque cookie ou traceur qui ne sert pas à fournir ou facturer des services de télécommunications. Le texte doit être adapté et prendre en compte le projet de règlement européen vie privée et communications. Les cookies techniques ou limités à une session et dont les données ne sont pas partagées ne doivent pas nécessiter de consentement. Des règles simples et claires sont nécessaires. |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |
| SME | | | | | |

## 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 : |
|---|---|
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |

## 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 : |
|---|---|
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |
| SME | |

**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 :** |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |
| SME | | |

# Révision de la LPD: des sanctions à contre-courant et à contre-raison

**Sylvain Métille,**
avocat[1].

**David Raedler ,**
avocat[2].

L'avant-projet n'accorde pas de réel pouvoir de sanction au Préposé fédéral à la protection des données. Cela va à l'encontre de l'évolution actuelle en Europe et affaiblit tant la position du Préposé que la protection des droits des personnes concernées.

## 1. Introduction

L'avant-projet de révision de la loi fédérale sur la protection des données (AP LPD), actuellement en consultation, a pour but de renforcer les droits de la personne dont les données sont traitées (la personne concernée) et, corolairement, les obligations du responsable du traitement (aujourd'hui appelé «le maître du fichier»). Un niveau de protection similaire à celui nouvellement introduit dans l'UE avec l'entrée en vigueur du Règlement général de protection des données (RGPD) sera assuré, de même que la reprise nécessaire de l'Acquis de Schengen.

De nombreuses obligations, tant nouvelles que préexistantes, viennent ainsi s'imposer au responsable du traitement, dont plusieurs devoirs d'information, de documentation et d'annonce[3]. Les atteintes à la sphère privée de la personne concernée, tout comme la violation des obligations précitées, s'accompagnent de sanctions. Ces dernières ne s'articulent toutefois pas autour d'un régime uniforme mais, au contraire, s'inscrivent tant en droit pénal que civil et administratif. Les autorités compétentes pour en connaître dépendent également du droit applicable comme nous le verrons ci-après, ce qui n'est guère satisfaisant.

## 2. Décisions et sanctions prévues par l'AP LPD

Le régime de décisions et de sanctions dans l'AP LPD se répartit entre les domaines administratif, pénal et civil.

En matière administrative tout d'abord, l'AP LPD innove par rapport à la réglementation actuelle en étendant certains des pouvoirs du Préposé fédéral à la protection des données et à la transparence (PFPDT). En particulier, l'art. 41 AP LPD lui confère un réel pouvoir d'enquête dès le moment où des indices font penser qu'un traitement de données pourrait être contraire à la loi[4]. Cela s'accompagne, là également comme innovation, d'une réelle obligation de collaborer des personnes impliquées et d'un pouvoir d'inspection des locaux sans avis préalable. Ces caractéristiques ne sont pas sans rappeler, toutes proportions gardées, les règles qui existent en droit de la concurrence (obligation de renseigner de l'art. 40 LCart et perquisitions selon l'art. 42 al. 2 LCart) ou, pour l'obligation de collaborer, en droit des marchés financiers (art. 29 LFINMA).

En ligne avec ces nouveaux pouvoirs, le PFPDT dispose également de la compétence de rendre de réelles décisions contraignantes, à la fois provisionnelles (art. 42 AP LPD) et au fond (art. 43 AP LPD)[5]. Il peut, en particulier, ordonner la suspension, la modification ou la cessation d'un traitement, la destruction de tout ou partie de données ou encore la suspension ou l'interdiction d'une communication de données à l'étranger. Cette nouvelle possibilité est un renforcement (partiel) du statut du PFPDT et un alignement (partiel) sur les pouvoirs dont disposent ses homologues européens[6].

A l'inverse, en revanche, le PFPDT ne dispose d'aucun réel pouvoir de sanction. Cela s'inscrit à contre-courant du régime européen[7] et pourrait bien ne pas être conforme à la Conven-

tion 108 du Conseil de l'Europe. Le PFPDT ne peut en effet pas sanctionner lui-même une violation du droit de la protection des données qu'il constaterait par son enquête, ni même le non-respect de ses propres décisions contraignantes. Confronté à de telles situations, il devra dénoncer l'affaire au Ministère public en vue d'enclencher une procédure pénale sur laquelle il n'aura plus aucune maîtrise[8]. Le Rapport explicatif justifie ceci essentiellement par les modifications dans l'organisation du PFPDT que cela aurait imposé, sur le modèle de la Comco, afin de «garantir la légitimité et l'acceptance *[sic]* des décisions ainsi que le respect des droits fondamentaux des personnes concernées»[9].

Le deuxième volet de décisions et de sanctions arrêtées dans l'AP LPD s'inscrit donc en droit pénal. De nombreuses hypothèses y sont prévues dans lesquelles le responsable du traitement peut être sanctionné pénalement lorsqu'il enfreint ses obligations. Il s'agit en particulier des obligations d'informer, liées au droit d'accès de la personne concernée, de communications destinées au PFPDT ou encore en lien avec les devoirs de diligence. Ces conséquences pénales joueront également un rôle central lorsque le responsable du traitement ne se conforme pas aux décisions (administratives) du PFPDT ou refuse sa collaboration lors d'une enquête (art. 50 al. 2 let. c et e AP LPD).

Ces éléments constituent (sous l'angle pénal) un renforcement significatif par rapport à la situation actuelle, dans laquelle les violations ne demeurent que peu sanctionnées. Une personne individuelle au sein de l'entreprise pourra ainsi être poursuivie pénalement et sera passible d'une amende allant jusqu'à 500 000 fr. (250 000 fr. en cas de négligence)[10]. Conformément aux règles habituelles de droit pénal, cette amende sera inscrite au casier judiciaire de la personne dès qu'elle atteint le montant de 5000 fr. Si l'identification de la personne responsable au sein de l'entreprise implique des mesures disproportionnées, l'entreprise pourrait être elle-même condamnée au paiement d'une amende, dont le montant est toutefois plafonné à 100 000 fr. (art. 53 AP LPD).

Sous l'angle civil enfin, la personne concernée disposera comme aujourd'hui de plusieurs voies d'action permettant d'assurer la mise en œuvre correcte de ses droits. Il s'agit des prétentions fondées sur la protection de sa personnalité, qui lui permettent entre autres d'interdire un certain traitement de données et de requérir la rectification de données erronées (art. 25 AP LPD[11]) ainsi que des actions en exécution de ses droits lorsque le responsable du traitement n'y donne pas correctement suite, dont son droit d'accès (art. 20 AP LPD). A la différence des prétentions fondées sur les droits de la personnalité toutefois, les actions en exécution de droits ne sont étonnamment pas expressément mentionnées dans l'AP LPD, tout en étant effleurées au contour du Rapport explicatif[12].

Indépendamment de la valeur litigieuse de l'action, l'AP LPD prévoit dans tous les cas l'application de la procédure simplifiée (art. 243 ss CPC) et, ce qui est nouveau, la gratuité de la procédure de conciliation et au fond (nouveaux art. 113 al. 2 let. g et 114 let. f CPC). L'action collective n'a en revanche pas été retenue. Sur ce dernier point d'ailleurs, l'AP LPD a raté, à notre sens, une possibili-

[1]Dr en droit, également chargé de cours l'Université de Lausanne.

[2]Egalement vice-président du Tribunal de prud'hommes de la Broye et du Nord vaudois.

[3]On peut, de façon très résumée, distinguer cinq catégories d'obligations nouvelles que sont les devoirs étendus d'information (art. 13 et 15 AP LPD), de documentation (art. 19 AP LPD) et d'annonce des violations intervenues (art. 19 AP LPD), une obligation de mener une analyse d'impact préalable (art. 16 AP LPD) ainsi que les principes de la protection des données dès la conception et par défaut (art. 18 AP LPD). Ces nouvelles obligations viennent s'ajouter à d'autres qui sont reprises de la LPD actuellement en vigueur (et en partie modifiée), notamment en matière de droit d'accès de la personne concernée (art. 20 à 22 AP LPD).

[4]Ce faisant, l'AP LPD ne restreint donc plus les pouvoirs du PFPDT par rapport aux personnes privées à un simple «établissement des faits» accompagné de recommandations, principalement limités par ailleurs aux cas d'erreur de système.

[5]Le régime actuel permet uniquement au PFPDT de saisir le Tribunal administratif fédéral afin d'y requérir le prononcé d'une décision contraignante.

[6]Le Rapport explicatif, ch. 1.4.2.4, les présente lui-même tant comme un renforcement qu'un alignement.

[7]Ce qualificatif de «contre-courant» étant expressément utilisé dans le Rapport explicatif, ch. 8.1.8.

[8]En particulier, l'art. 50 al. 2 let. e AP LPD sanctionne de l'amende le non-respect d'une décision signifiée par le PFPDT; pour ce renvoi explicitement, cf. Rapport explicatif, ch. 8.1.7.7 in fine.

[9]Rapport explicatif, ch. 8.1.8. On peut néanmoins s'étonner de cette réserve relative aux droits fondamentaux des personnes concernées, dans la mesure notamment où l'AP LPD opère un renvoi explicite à la PA pour ce qui a trait à l'enquête du PFPDT (art. 44 al. 1 AP LPD), caractéristique qui devrait en tout cas assurer la protection des droits de procédure des parties.

[10]Cela reste modeste en comparaison des amendes administratives prévues par l'art. 83 RGPD qui pourront s'élever, selon la catégorie de l'infraction, de 10 ou de 20 millions d'euros ou, dans le cas d'une entreprise, de 2% à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

[11]Une règle en partie proche, sans référence aux bases légales des art. 28 ss CC, est prévue à l'art. 34 AP LPD dans le cas des traitements de données effectués par un organe fédéral.

[12]Cf. la référence unique aux actions en exécution du droit de consultation et à l'effacement de l'art. 12 AP LPD ainsi qu'à l'action en exécution du droit d'accès de l'art. 20 AP LPD, séparée expressément des actions selon l'art. 25 AP LPD, au ch. 8.2.9.1 du Rapport explicatif.

té qui aurait été utile. Le Rapport explicatif mentionne tout de même cette éventualité, qu'il écarte au motif d'un traitement devant se faire plus largement[13]. Pourtant, une telle éventualité aurait également permis de simplifier la procédure et d'étendre utilement les droits de chacun des lésés.

## 3. Appréciation critique

L'absence d'un pouvoir de sanction du PFPDT est regrettable. Cela aurait en effet été la preuve de son indépendance et aurait permis d'instaurer un régime de sanctions uniforme à travers la Suisse, sans que des variations de pratique se posent selon les cantons. Justifié par cette absence de sanctions administratives, le «renforcement» des sanctions pénales laisse pour sa part songeur pour au moins cinq raisons.

Premièrement, les amendes maximales sont largement inférieures à celles prévues dans les pays voisins[14].

Deuxièmement, ces sanctions visent pour l'essentiel une personne individuelle (bouc émissaire?) alors que c'est, au final, l'entreprise qui devrait être principalement responsable du traitement de données effectué en son sein.

Troisièmement, et en tout cas si les dispositions pénales ainsi prévues sont correctement mises en œuvre, les autorités pénales risquent d'être saisies d'un grand nombre d'affaires. Or, leurs moyens étant limités, ces affaires risquent de ne pas être une priorité. Il est également envisageable que ces affaires ne soient pas traitées avec les compétences nécessaires, les autorités pénales n'étant pas particulièrement spécialisées dans le domaine de la protection des données.

Quatrièmement, le PFPDT ne sera pas partie aux procédures pénales qu'il enclencherait, et ne pourra donc en assurer le suivi. Il ne pourra non plus, de ce fait, y défendre l'existence d'une violation de la loi ou d'une de ses décisions. Pourtant, il aura le plus souvent déjà ouvert une procédure administrative, instruit les faits en détail et, potentiellement, inspecté directement les locaux de la personne visée. Malgré la connaissance ainsi acquise du dossier, il en perdra la maîtrise dès le moment où il souhaite qu'une sanction soit prononcée.

Cinquièmement enfin, l'existence de procédures administratives et pénales parallèles, auxquelles pourra venir s'ajouter une procédure civile ouverte par la personne concernée, amènera les personnes impliquées (dont le responsable du traitement) à devoir faire face en même temps à plusieurs procédures et, par-là, à plusieurs autorités différentes.

Le système prévu implique donc une multiplication des procédures et des formalités nécessaires pour assurer le respect du droit de la protection des données.

D'une part, la personne concernée ne pourra pas se contenter de se raccrocher aux éventuels actes d'enquête qui seraient mis en œuvre par le PFPDT et y faire valoir ses droits. L'art. 44 al. 2 AP LPD précise en effet expressément que seule la personne privée contre qui une enquête est ouverte bénéficie de la qualité de partie, à l'exclusion donc de la personne concernée. Cette caractéristique, qui vaut y compris lorsque l'enquête a été ouverte sur sa dénonciation[15], l'oblige donc à procéder par la voie civile et éventuellement pénale[16].

D'autre part, le responsable du traitement devra aussi faire face à «l'éclatement» des procédures, cette fois entre les trois volets administratif, civil (à l'égard de la personne concernée) et pénal, ce dernier pouvant être enclenché non seulement par une plainte de la personne concernée, mais également suite à la dénonciation du cas par le PFPDT.

Les problèmes posés par cette multiplication des compétences et voies de droit peut être mise en évidence par un exemple simple. L'exploitant d'un fitness met en place, à l'insu de ses clients, un système d'analyse de leurs préférences par le biais d'une carte d'identification qu'ils doivent porter en tout temps et qui enregistre tous les détails des séances d'entraînement (machine utilisée, durée de l'entraînement, effort fourni, etc.). L'exploitant utilise ensuite ces données afin d'envoyer des publicités ciblées à ses clients et les vend à une entreprise américaine de compléments alimentaires de même qu'à une assurance maladie. Enfin, interrogé par trois clients, il conteste tout enregistrement de données et refuse tout droit d'accès.

Dans cet exemple, l'exploitant du fitness enfreint notamment les principes de proportionnalité, finalité et protection des données par défaut. Il viole également les règles sur la communication de données à l'étranger, le devoir d'informer lors de la collecte et en cas de communication à un tiers, et l'exercice du droit d'accès. Il n'a pas non plus effectué d'analyse d'impact, malgré les risques entraînés par le système. Plusieurs atteintes à la

personnalité des personnes concernées selon l'art. 23 AP LPD en découlent directement[17].

Malgré une situation simple et unique, les voies d'action seront «éclatées»:

- le PFPDT pourra mener une enquête, procéder à l'inspection des locaux et prononcer une interdiction du traitement ainsi que du transfert à l'étranger, dans le cadre d'une procédure administrative;
- le PFPDT devra dénoncer l'affaire au Ministère public, ce qui ouvrira, en parallèle, une procédure pénale pour que l'exploitant du fitness soit sanctionné;
- les clients souhaitant agir à l'encontre du fitness devront, pour leur part, agir par une procédure civile[18], chacun séparément.

Ces trois procédures seront pour l'essentiel indépendantes l'une de l'autre, tout comme les autorités appelées à intervenir. Alors même qu'un éventuel rapport du PFPDT pourrait être pris en compte, chaque autorité pourra instruire les faits à sa manière et interpréter différemment les actes commis. Le risque existe donc qu'un même état de fait soit perçu par le PFPDT comme constitutif d'une grave violation de la loi, alors qu'un juge pénal et/ou civil le refuserait.

L'existence d'un pouvoir de sanction du PFPDT aurait pourtant pu simplifier ce processus. Il aurait, en effet, pu directement **(i)** ouvrir une enquête à l'encontre de l'exploitant du fitness, **(ii)** rendre une décision lui faisant interdiction de récolter, de traiter et de transmettre les données à l'étranger et **(iii)** le sanctionner pour les infractions commises[19]. Cette solution présenterait l'avantage d'exclure un éclatement en deux volets, administratif et pénal, et offrirait potentiellement un traitement plus rapide, plus spécialisé et non contradictoire.

## 4. La Comco et la Finma comme inspiration?

Le rôle du PFPDT n'est pourtant pas si différent de ce que l'on connaît en droit de la concurrence et en droit des marchés financiers, deux domaines se caractérisant à la fois par l'existence d'une autorité administrative, un fort risque de sanctions ainsi que l'existence en parallèle de volets pénal, administratif et (en partie du moins) civil.

En droit de la concurrence, la Comco dispose d'un fort pouvoir de sanctions sur le plan administratif, prévu aux art. 49a ss LCart. Cette compétence lui permet notamment de condamner une entreprise ayant enfreint la LCart au paiement d'un montant pouvant aller jusqu'à 10% du chiffre d'affaires réalisé en Suisse au cours des trois derniers exercices. Prononcée par la Comco, cette sanction est prise sur la base des faits instruits par le secrétariat, d'entente avec un membre de la présidence (art. 53 LCart). En parallèle, la LCart prévoit également un nombre limité de sanctions pénales, qui visent toutefois uniquement la violation des accords amiables, décisions administratives et autres décisions des autorités de la concurrence. Des prétentions civiles peuvent enfin toujours être soulevées par une personne lésée par la restriction à la concurrence[20].

Formellement, la Comco (qui prononce les sanctions administratives) et le secrétariat (qui instruit les faits) constituent deux entités distinctes, compo-

[13]Rapport explicatif, ch. 1.6.3.

[14]Cf. note 10. Les Etats membres peuvent en outre introduire des sanctions pénales additionnelles (art. 84 RGPD).

[15]Cette précision est expressément faite dans le Rapport explicatif, ch. 8.1.7.8.

[16]Idem.

[17]Ce point est d'autant accentué par le fait que les données récoltées peuvent être qualifiées de sensibles (en tant qu'elles portent sur la santé des clients) et constituer une forme de profilage au sens de l'art. 3 let. f AP LPD.

[18]Ils pourront également eux-mêmes porter plainte et amener l'affaire par-devant le Ministère public, en quel cas l'affaire devrait en principe être jointe à la procédure dénoncée par le PFPDT pour les mêmes faits.

[19]La possibilité de participer à la procédure pourrait également être donnée aux personnes concernées, individuellement ou collectivement, afin notamment d'assurer au mieux le caractère complet de l'instruction.

[20]Le CPC prévoit d'ailleurs, dans ce cas, une instance cantonale unique selon son art. 5 al. 1 let. b.

[21]Cf. à ce sujet notamment l'art. 1 du Règlement interne COMCO.

sant ensemble les autorités de la concurrence[21]. Il y a donc bien une séparation institutionnelle entre l'autorité d'enquête et celle de décision. Leurs compétences demeurent toutefois fortement imbriquées. L'ouverture d'une enquête et la réalisation d'actes d'instruction par le secrétariat doit notamment intervenir d'entente avec un membre de la présidence de la Comco[22]. De plus, bien que la direction du secrétariat soit nommée par le Conseil fédéral, les autres membres du personnel le sont par la Comco (art. 24 al. 1 LCart et art. 10 al. 2 let. c Règlement interne Comco).

En droit des marchés financiers, la situation est en partie différente. De façon plus proche de ce qui est prévu dans l'AP LPD, le système de sanction y est principalement axé sur le droit pénal. Les art. 44 ss LFINMA arrêtent ainsi plusieurs infractions couvrant à la fois les violations des lois sur les marchés financiers et le non-respect des décisions de la Finma, qui s'ajoutent aux suites pénales prévues dans d'autres lois spéciales. Du point de vue civil, toutes prétentions liées aux violations du droit des marchés financiers sont totalement disjointes de la réglementation administrative.

La Finma ne sanctionne donc pas elle-même monétairement des entreprises ou des personnes qui enfreindraient l'une ou l'autre des lois sur les marchés financiers. Elle dispose de très forts pouvoirs d'instruction et d'enquête, notamment par la possibilité de mandater ou d'imposer un expert chargé d'intervenir directement au sein de l'assujetti et d'y contrôler le respect des obligations légales[23]. Elle peut également prendre des mesures directement contre un assujetti ou une personne physique impliquée dans les faits en vue du rétablissement de l'ordre légal (art. 31 LFINMA), notamment en prononçant une interdiction d'exercer (art. 33 LFINMA), en confisquant le gain acquis (art. 35 LFINMA) ou encore en retirant l'autorisation d'exercer d'un assujetti (art. 37 LFINMA). Ces mesures peuvent être publiées par la FINMA, avec les références personnelles des assujettis (art. 34 al. 1 LFINMA). S'y ajoutent encore d'autres mesures spécifiquement prévues par les autres lois sur les marchés financiers.

Nonobstant l'absence de sanctions administratives monétaires, la Finma dispose donc de très larges pouvoirs, pouvant, en substance, aller jusqu'à un droit de vie ou de mort sur l'assujetti. Afin d'assurer une indépendance nécessaire au processus d'instruction et de décision, la fonction d'«enforcement» est séparée de celle de surveillance au sein de la Finma, chacune étant confiée à des divisions différentes[24].

## 5. Quelles leçons en tirer?

La comparaison entre l'AP LPD et les deux systèmes décrits permet de constater l'absence de réels pouvoirs contraignants du PFPDT. Quand bien même il bénéficie, sur le papier, d'un fort pouvoir d'enquête et de la possibilité de rendre des décisions contraignantes, il se voit priver, dans les faits, de toute possibilité de s'assurer lui-même d'une correcte mise en œuvre de ses décisions ou d'une poursuite complète des infractions au droit de la protection des données. Il en est réduit à «menacer» le responsable du traitement de suites pénales théoriques, afin d'espérer avoir un poids dans l'application de l'AP LPD. Or, rien ne lui garantit que l'autorité pénale donnera correctement suite à sa dénonciation.

Cela constitue clairement une situation plus faible en comparaison à la Comco, dont les forts pouvoirs d'instruction et de sanction administrative confèrent un poids prépondérant dans l'application du droit de la concurrence. Il en est toutefois de même également par rapport à la Finma, cela même en l'absence d'un risque direct de sanctions monétaires pour les assujettis. Ses décisions peuvent en effet avoir une énorme incidence à leur égard et pour les personnes physiques impliquées, notamment en cas d'interdiction d'exercer et de retrait d'une autorisation.

L'argument, posé dans le Rapport explicatif, selon lequel le PFPDT ne pourrait avoir un pouvoir de sanction qu'à la condition que son organisation soit totalement revue, ne constitue, selon nous, pas un obstacle justifiant de l'en priver.

Premièrement, un modèle similaire à la Comco pourrait être suivi et serait, dans un tel contexte, à même d'assurer le respect de la LPD. Il suffirait, en effet et cas échéant, d'opérer structurellement une différence en prévoyant deux «autorités de la protection des données», soit le PFPDT et son secrétariat. S'il devait représenter quelques coûts supplémentaires pour l'Etat, il faut garder en perspective que l'AP LPD va générer une importante charge nouvelle pour les autorités pénales cantonales.

Deuxièmement, et sans même opérer une telle modification structurelle, un pouvoir de sanction pourrait aussi être donné au PFPDT en s'inspirant du régime existant pour la Finma. Plusieurs des mesures prononcées par cette autorité (dont l'interdiction d'exercer et le retrait de l'autorisation) correspondent, dans les faits à de véritables sanctions. Pourtant, c'est bien toujours la Finma elle-même (par ses différentes divisions et la direction) qui instruit et rend le prononcé en question.

Troisièmement enfin, et dans tous les cas, il convient de rappeler que le PFPDT représente bien une autorité indépendante. Il ne s'agit ainsi, par exemple, pas d'un chef de département ou d'une entité soumise aux instructions d'autres parties de l'administration. En ce sens donc, il est parfaitement à même d'assurer l'indépendance du processus et le respect des droits fondamentaux des personnes impliquées.

Au final, l'unification de certains pouvoirs d'instruction et de sanction en main du PFPDT garantirait une uniformité de la procédure et une application correcte du droit de la protection des données. Seule cette solution offrirait à ce domaine l'importance qui devrait lui revenir. On ose espérer que la procédure de consultation en cours permettra de retravailler le projet actuel en ce sens et de soumettre au Parlement une version remodelée.

[22]Seule une enquête préalable peut être décidée par le secrétariat lui-même (art. 26 et 27 LCart).

[23]Cela peut se faire essentiellement par le biais d'une société d'audit, d'un chargé d'audit ou d'un chargé d'enquête (art. 24, 24a et 36 LFINMA).

[24]Cf. art. 18 du Règlement d'organisation Finma.

**Amstutz Jonas BJ**

---

**Von:** Markus Mohler <markushfmohler@bluewin.ch>
**Gesendet:** Freitag, 10. März 2017 12:44
**An:** Amstutz Jonas BJ
**Betreff:** Revison DSG, kurze Stellungnahme
**Anlagen:** Diskriminierende Personenkontrollen_ Verfassungs- und verwaltungsrechtliche Vorgaben Rechtslage und Praxis.pdf

**Wichtigkeit:** Hoch

Sehr geehrter Herr Amstutz,

wiewohl nicht Spezialist in datenrechtlichen Fragen, erlaube ich mir eine kurze Stellungnahme zu Art. 3 Bst. c Ziff. 2 des VE DSG im Rahmen des Vernehmlassungsverfahrens:

Danach gehören zu den besonders schützenswerten Personendaten u.a.
«Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie»
Aus zweierlei Gründen erscheinen mir die Eigenschaften «Rasse» und «Ethnie» als fragwürdig in Bezug auf besonders schützenswerte Personendaten:

1. Der Begriff «Rasse» wird in der gesamten Rechtswissenschaft als unhaltbar, in der Kulturanthropologie als unbrauchbar bezeichnet. Dennoch ist er bekanntlich Anknüpfungskriterium im Diskriminierungsverbot nach Art. 8 Abs. 2 BV. Ich habe dazu eben einen Aufsatz publiziert, der sich eingehend mit den Begriffen «Rasse» und Ethnie» aus rechtlicher Sicht auseinandergesetzt (Anhang). Im Zusammenhang mit dem Verweis auf die EU DS-GVO erscheint «Rasse» insofern schon als eigenartig, als die EU Theorien, welche die Existenz verschiedener menschlicher Rassen zu belegen versuchen, in einem Erlass (!) ausdrücklich zurückweist (Richtlinie 2000/43/EG, ABl. L 180 b. 19. Juli 2000, 22ff.). Ebenso unbestimmt ist der Begriff «Ethnie». Für beide Begriffe zeigen schon Menschen mit Eltern unterschiedlicher Herkunft die Unbrauchbarkeit. Daraus ergibt sich auch ein Widerspruch zur nachfolgenden Ziff. 4: «biometrische Daten, die eine natürliche Person eindeutig identifizieren». Weder «Rasse» noch «Ethnie» vermögen dies. Ginge es mit der Aufnahme von «Rasse» und «Ethnie» ausschliesslich um die Verhinderung von Diskriminierungen, genügte an sich auch die BV (als direkt anwend- bzw. anrufbares Grundrecht), wenngleich auf höchst fragwürdige Art.
2. Was mit «Rasse» und «Ethnie» gemeint sein soll, sind *äusserlich erkennbar Merkmale*. Kann eine menschliche Eigenschaft, die sich als jederzeit äusserlich erkennbares Merkmal zeigt, ein besonders schützenswertes Personendatum sein? Wohl kaum. Dann gehörten ja auch die Körpergrösse oder der Leibesumfang dazu, was wohl nicht gemeint wäre. Aber beides sind ebenso klar äusserlich erkennbare äusserliche Merkmale. Die Körpergrösse gehörte auch zu den Unterscheidungsmerkmalen, die nach bundesgerichtlicher Definition «einen wesentlichen und nicht oder nur schwer aufgebbaren Bestandteil der Identität der betroffenen Person ausmachen» (BGE 139 I 292, E. 8.2.1).

Mit andern Worten sollte m.E. auf diese beiden Begriffe verzichtet werden. Sie scheinen lediglich aus Gründen der (vermeintlichen) politischen Korrektheit als Gesetzestext fortbestehen zu sollen, wie wohl diese selber gerade vermieden werden müssten.

Eine andere Möglichkeit könnte der Begriff *«Abstammung»* sein. Damit vermiede man zumindest die untauglichen Begriffe «Rasse» und «Ethnie». Umgekehrt würden beispielsweise auch Menschen erfasst, die ausserehelich gezeugt, von (auch gleichgeschlechtlichen) Partnern adoptiert worden sind oder von Eltern unterschiedlicher oder selbst unbestimmter «ethnischer» Herkunft stammen, was dann tatsächlich nicht notwendigerweise äusserlich erkennbar ist, aber zu den wirklich schützendwerten Personendaten gehörte.
Es könnte viele Beispiele angeführt werden, welche auch den Begriff «Ethnie» oder «ethnische Herkunft» in aller Deutlichkeit als absurd erscheinen lassen.

Mit freundlichen Grüssen
Markus Mohler

Dr.iur.Markus H.F. Mohler
ehem. Lehrbeauftragter für öffentliches,
speziell Sicherheits-und Polizeirecht
an den Unis von Basel und St. Gallen
Im Wiesengrund 5
4102 Binningen-Basel
Tel.: +4161 422 1347
Mobile: +4179 669 1474
markushfmohler@bluewin.ch
www.recht-sicherheit.ch

Jusletter

# Diskriminierende Personenkontrollen: Verfassungs- und verwaltungsrechtliche Vorgaben – Rechtslage und Praxis

Autor: Markus H. F. Mohler

Beitragsarten: Beiträge
Rechtsgebiete: Öffentliches Recht, Verwaltungsrecht
Zitiervorschlag: Markus H. F. Mohler, Diskriminierende Personenkontrollen: Verfassungs- und verwaltungsrechtliche Vorgaben – Rechtslage und Praxis, in: Jusletter Next: 6. März 2017

Das Diskriminierungsverbot in Art. 8 Abs. 2 der Bundesverfassung stützt sich u.a. auf Anknüpfungskriterien wie «Rasse» und (ethnische) Herkunft. Diese Ausdrücke werden von der Kulturanthropologie aber als unbrauchbar, von der Rechtswissenschaft als unhaltbar bezeichnet. Dennoch wird in diesem Zusammenhang an ihnen festgehalten. Andere objektive Kriterien und der Einbezug der subjektiven Seite könnten mit deutlicheren Vorgaben bessere Ergebnisse zeitigen. Dabei stellt die Plausibilität eines vernünftigen Anfangsverdachts ein wesentliches Element dar. Es liegt in der Verantwortung der Politik, nicht für mehr, sondern besseres Recht zu sorgen.

## Inhaltsverzeichnis

> «Die kulturellen Faktoren beeinflussen den Menschen bis ins Körperliche, die biologischen Faktoren beeinflussen in selbst im kulturellen Bereich. Darum bleibt ein Unrecht, das dem Menschen zugefügt wird, nie begrenzt. Es ist immer total. Daher die Zwiespältigkeit des Rassenproblems, das zugleich Tatsache ist, Vorwand und Schande.»
> (Jeanne Hersch)

## Vorbemerkung [1]

[Rz 1] Das Schweizerische Kompetenzzentrum für Menschenrechte, seit 2011 Projekt eines praxisorientierten Dienstleistungszentrums im Rahmen eines universitären Netzwerkes, [2] führte am 1. Dezember 2016 in Bern eine polizeirechtliche Fachtagung zum Thema Diskriminierende Personenkontrollen aus praktischer, juristischer und sozialwissenschaftlicher Perspektive durch. Der Themenbereich Polizei und Justiz des SKMR ist innerhalb dieses Netzwerkes bei der Juristischen Fakultät der Universität Bern angesiedelt. [3]

[Rz 2] Wiewohl das Thema des Einleitungsreferates auf die relevanten Grundlagen in der schweizerischen Rechtsordnung fokussiert, bedarf es eines kurzen Blicks über die grundlegende Bedeutung der in diesen Erlassen und in diesem Zusammenhang verwendeten Begriffe hinaus. Dieser Blick drängte sich auch aus der zweiten, der sozialwissenschaftlichen Tagungsperspektive auf. Denn die buchstäbliche quasi-Selbstverständlichkeit [4] verwendeter Ausdrücke als Rechtsbegriffe im Alltag beruht auf einem überaus unsicheren Fundament. Beschränkt ist die Betrachtung auf Unterscheidungsmerkmale, die als Grundtypen des Verbotes der Diskriminierung nach «Rasse» bzw. «Ethnie» oder «ethnische Herkunft» gelten. Sodann fokussiert die Diskussion auf Personenkontrollen als intervenierende Realakte, [5] die selber ein spezifisches Wesensmerkmal des Polizeirechts im Unterschied zum sonstigen Verwaltungsrecht bilden.

[Rz 3] Die Perspektive des UNO-Ausschusses gegen Rassendiskriminierung (Committee on the Elimination of Racial Discrimination, CERD) wurde in einem weiteren Referat [6] behandelt.

# I. Zum Begriff «Diskriminierung»

## 1. Etymologie und völkerrechtlicher Bezug

[Rz 4] Der Ausdruck ist in der deutschen Sprache heute nur negativ konnotiert. Etymologisch ist das so nicht richtig. «Diskriminieren» kommt von lat. «discriminare», d.h. unterscheiden, trennen, und von «discrimen», d.h. das Scheidende, die Trennlinie. [7] Im Französischen, Italienischen und Englischen ist dies nicht so: in diesen Sprachen bedeuten die Nachfolgewörter (discriminer, discriminare, discriminate) nach wie vor «unterscheiden», unterschiedlich behandeln, zunächst ohne wertenden Zusatz. [8]

[Rz 5] Es handelt sich um einen ursprünglich politischen Begriff, der über Art. 14 EMRK[9, 10], Art. 2 und 10 des UNO Pakts I[11], Art. 24 und 26 UNO Pakt II[12] sowie das Internationales Übereinkommen zur Beseitigung jeder Form von Rassendiskriminierung[13] zu einem (verfassungs-) rechtlichen geworden ist.[14]

## 2. In der BV

[Rz 6] In der Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) kommt der Ausdruck ausschliesslich in Art. 8 Abs. 2 vor im Zusammenhang mit den aufgelisteten Merkmalen[15] in Bezug auf Menschen. Das Diskriminierungsverbot war bereits impliziter Teilgehalt von Art. 4 BV 1874.[16]

[Rz 7] Unterschieden wird vorab zwischen einem formalen, primär an den nicht abschliessend («namentlich»)[17] genannten Merkmalen orientierten Diskriminierungsbegriff, und einem materiellen Diskriminierungsbegriff. Dem formalen Begriff wird in der Literatur mehrheitlich nicht gefolgt.[18] Auch in der Umschreibung des materiellen Diskriminierungsbegriffs zeigen sich Unterschiede (dazu nachfolgend, Rz. 12 ff.). Ein Kennzeichen des materiellen Verständnisses ist dessen Bezug auf das Ergebnis einer Behandlung und nicht auf die Behandlung selber. Dieses verpönte Ergebnis und seine causa sind allerdings ihrerseits zu definieren. Darauf wird zurückzukommen sein (Rz. 45 ff.).

[Rz 8] Das in der BV in Übereinstimmung mit dem Völkerrecht festgeschriebene Verbot der Diskriminierung ist zunächst nicht als isolierte Bestimmung zu interpretieren. Es ist dogmatisch gesehen Teil des Gleichbehandlungsgebotes (Art. 8 Abs. 1 BV)[19] und steht in direktem Zusammenhang mit der Menschenwürde (Art. 7 BV)[20], dem Willkürverbot (Art.9 BV)[21] sowie der persönlichen Freiheit (Art. 10 Abs. 2 BV). Diskriminierung ist aber nicht gleichbedeutend mit Rechtsungleichbehandlung.[22] Nicht jede nach dem allgemeinen Gleichheitssatz sachwidrige Unterscheidung ist eine Diskriminierung.[23]

[Rz 9] Die Vielfalt der Definitionen (samt deren Strukturierung) von Diskriminierung und die Unterschiede in der Benennung, was das Ziel des Diskriminierungsverbotes sei, ist beeindruckend, aber nicht notwendigerweise hilfreich für die Praxis. Es sei eine vereinfachende Übersicht gewagt:

[Rz 10] Das Diskriminierungsverbot weist zunächst zwei Schutzrichtungen auf: ein Benachteiligungs- und ein Anknüpfungsverbot.[24] Es stellt eine Konkretisierung und Verstärkung des Gleichbehandlungsgebotes dar,[25] eine Qualifizierung hinsichtlich der Anknüpfungstatbestände. Jede Differenzierung nach einem der verpönten Merkmale ist zwar nicht absolut verboten,[26] erscheint aber von vorneherein fragwürdig:[27] «Das Diskriminierungsverbot gemäss Art. 8 Abs. 2 BV schliesst indes die Anknüpfung an ein verpöntes Merkmal - wie beispielsweise Herkunft, Rasse, Geschlecht, soziale Stellung oder religiöse Überzeugung - nicht absolut aus. Eine solche begründet zunächst lediglich den blossen Verdacht einer unzulässigen Differenzierung».[28] Eine Abweichung vom Prinzip der absoluten Gleichbehandlung ist somit nur ausnahmsweise in qualifizierter Weise im Zusammenhang mit besonderen sachlichen Gegebenheiten zulässig.[29] Welcher Art einer Ungleichbehandlung in diesem Zusammenhang als besondere sachliche Gegebenheit zu genügen vermag, unterliegt im Einzelfall kontroversen Beurteilungen (vgl. nachfolgend IV. und V.)

[Rz 11] Das Bundesgericht definiert in konstanter Rechtsprechung Diskriminierung wie folgt: «Eine Diskriminierung liegt vor, wenn eine Person ungleich behandelt wird allein aufgrund ihrer Zugehörigkeit zu einer bestimmten Gruppe, welche historisch oder in der gegenwärtigen sozialen Wirklichkeit tendenziell ausgegrenzt oder als minderwertig angesehen wird. Die Diskriminierung stellt eine qualifizierte Ungleichbehandlung von Personen in vergleichbaren Situationen dar, indem sie eine Benachteiligung von Menschen bewirkt, die als Herabwürdigung oder Ausgrenzung einzustufen ist, weil sie an Unterscheidungsmerkmalen anknüpft, die einen wesentlichen und nicht oder nur schwer aufgebbaren

Bestandteil der Identität der betroffenen Personen ausmachen; insofern beschlägt das Diskriminierungsverbot auch Aspekte der Menschenwürde nach Art. 7 BV». [30] Dabei geht es von der Prämisse der notwendigen Verbindung von Anknüpfungskriterien (Benennung einer Person als zu einer Gruppe als «Kategorie» gehörig) und der Ungleichbehandlung aus. [31] Vom Sozial- und Rechtswissenschaftlichen her ist das – zumindest ausserhalb des Strafrechtsbereichs – insofern fragwürdig, als es gegenüber nach diesen Kategorien keineswegs unterscheidbaren Personen ebenso diskriminierende Verhaltensweisen im Sinne der Ausgrenzung (aktuelles Problem: Personenfreizügigkeit [32]) oder (vermeintliche) Ungleichbehandlungen gibt. [33] Damit können Abgrenzungen noch heikler werden. [34, 35]

[Rz 12] Bernhard Waldmann hält auch die bisher vertretenen materiellen Diskriminierungsbegriffe für nicht ganz überzeugend. Er postuliert daher einen eigenen, der die bisherigen v.a. verfeinert. Danach sei eine Diskriminierung als Angriff auf die Wertschätzung eines Menschen als Person zu verstehen. Vier Erkenntnisse seien damit verbunden:

- jede Diskriminierung sei immer in einem pejorativen Sinn zu verstehen,
- das Behandlungsergebnis sei allein massgebend, weshalb es auf eine allfällige Absicht nicht ankomme,
- die einen Menschen in seiner Würde beeinträchtigende Behandlung könne verschiedene Formen [36] annehmen und
- die Verfassungsverletzung liege bereits in der Beeinträchtigung der Wertschätzung als Person, weshalb es keines zusätzlichen Schadens bedürfe. [37]

[Rz 13] M.E. vermag auch diese Umschreibung nicht ganz zu überzeugen. Eine Wertschätzung ist erstens subjektiv definiert ist. Dass Diskriminierung stets im pejorativen Sinn zu verstehen sei, mag zunächst mit der im Deutschen einseitig negativen Konnotation von «diskriminieren» zusammenhängen (vorstehend Rz. 22) und beruht zweitens auf einer intendierten oder mindestens vorurteilsbehafteten Behandlungsweise. Drittens bleibt zu bestimmen, wer das Behandlungsergebnis worauf gestützt rechtsgenügend als diskriminierend beurteilt (vgl. dazu nachstehend Rz. 22). [38]

[Rz 14] Auch das Ziel des Diskriminierungsverbotes wird nicht ganz einheitlich umschrieben: Zum einen als gegen die Menschenwürde verstossende Schlechterbehandlung zufolge formalrechtlich genannter Eigenschaften oder Zugehörigkeiten, welche die betreffende Person nicht oder kaum ändern kann, [39] dann ebenso als Angriff auf die Wertschätzung eines Menschen als Person, die durch eine auch nicht beabsichtigte Behandlung im Ergebnis zum Ausdruck komme. Die konstituierenden Elemente der Wertschätzung seien, so Waldmann (unter Verweis auf Tschannen/Kiener), die Eigenschaften einer Person: die (1) ihre Identität bestimmten, (2) nicht oder zumindest nur schwer abänderbar seinen und (3) erhebliches Stigmatisierungspotential beinhalteten. [40] Menschenwürde und Wertschätzung einer Person müssen aber nicht deckungsgleich sein. Auch das Kriterium des Stigmatisierungspotentials ist zweifelhaft, da dies (der Willkür) der politischen Korrektheit eine rechtliche Definitionsmacht zuordnen könnte.

[Rz 15] Der objektive Sachverhalt der Diskriminierung setzt nach herrschender Lehre nicht voraus, dass die handelnde Person (oder der Gesetzgeber oder die Herausgeber von Dienstvorschriften) diskriminieren will. Dies kann bei unbewussten Vorurteilshaltungen zutreffen. [41] Ein Blick auf kulturanthropologische Ansätze (dazu nachfolgend, II. 1-3) eröffnet jedoch Zweifel hinsichtlich des gänzlichen Ausschlusses subjektiver Elemente bei der handelnden oder unterlassenden Person. Nach der hier vertretenen Auffassung kann auch rechtswissenschaftlich für das als konstitutiv bezeichnete Element der pejorativen Einschätzung, der Herabwürdigung, in den hier diskutierten Zusammenhängen nicht auf die subjektive Betrachtung [42] verzichtet werden.

[Rz 16] Umgekehrt muss sich die diskriminierte Person der Schlechterbehandlung aber nicht bewusst sein. [43]

[Rz 17] Schliesslich: Unterschieden wird zwischen direkter oder unmittelbarer und der mittelbaren Diskriminierung. Unmittelbar ist sie, wenn die Handlung, ein Erlass selber oder eine Dienstvorschrift eine Schlechterbehandlung (oder Privilegierung) in sich trägt. Als mittelbar wird eine Diskriminierung bezeichnet, wenn eine «neutrale» Regelung, die keine Benachteiligung von Personen, die nach bestimmten Merkmalen gegen Diskriminierung geschützt sind, enthält, in ihren Auswirkungen die Schlechterbehandlung nach solchen Kriterien oder Verfahren trotzdem ermöglicht, ohne dass dies sachlich begründet und verhältnismässig wäre. [44]

[Rz 18] Dieser kurze Überblick zeigt, dass selbst der verfassungsrechtliche Begriff der Diskriminierung eine erhebliche Unschärfe aufweist.

### 3. In den Kantonsverfassungen

[Rz 19] Nach diesen auch dogmatischen Feinheiten ist es interessant, auf die verwendeten Ausdrücke in den Kantonsverfassungen zu achten. In zehn Kantonsverfassungen findet sich der Ausdruck «diskriminieren» oder «Diskriminierung» im Sinne eines Verbotes. [45] In sieben Kantonsverfassungen werden die Ausdrücke «benachteiligen oder bevorzugen» im Sinne eines Verbotes verwendet. [46] Zwei Kantone begnügten sich mit Verweisen auf die Rechtsgleichheit [47] und einer mit dem Verweis auf die BV. [48]

[Rz 20] Da das Diskriminierungsverbot im Grundrechtskatalog der BV eingeordnet ist und demnach generell gilt, sind diese Unterschiede für die Rechtsverwirklichung unbedeutend. Umgekehrt scheint kein Kanton einen weitergehenden Diskriminierungsschutz zu enthalten (vgl. aber nachfolgend Rz. 36 betr. KV BS).

### 4. In den Polizeigesetzen der Kantone

[Rz 21] In keinem der kantonalen Polizeigesetze kommt der Ausdruck «diskriminieren» oder «Diskriminierung» vor. An nächsten kommen dem Diskriminierungsverbot in § 22 Polizeigesetz des Kantons Basel-Stadt [49] die Gelübde-Formel: «…meine Pflichten ohne Ansehen der Person, vorurteilslos und unbestechlich …zu erfüllen» [50] sowie in Art. 81 Abs. 3 des Polizeigesetzes des Kantons Jura [51] die etwas anders gefasste Formulierung «… interdit à tout agent de la police cantonale de faire subir à quiconque des traitements dégradants ou humiliants».

## II. Die Anknüpfungskriterien der «Rasse», «Ethnie» und «Hautfarbe» - ein kurzer Überblick

### 1. Zum Begriff der Rasse

[Rz 22] «Rasse» wird in der rechtswissenschaftlichen Literatur durchwegs als «problematisches» Kriterium, als soziales Konstrukt [52] oder soziale Kategorisierung, [53] oder auch als «wissenschaftlich unhaltbar» [54] bezeichnet. In der sozial- und kulturanthropologischen Literatur wird der Ausdruck ebenso als vom Naturwissenschaftlichen her unbrauchbar, [55] als ohne Bezug zu einem «vermeintlich naturwissenschaftlichem oder pseudo-wissenschaftlichen» Begriff [56] gewertet. [57] Rasse sei «not so much a biological phenomenon than a social myth». [58] Die EU weist Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, in einer Richtlinie aus dem Jahr 2000 explizit zurück. [59] Der Ausdruck wird umgekehrt jedoch für die Bezeichnung von sensiblen, zweifelhaften bzw. inakzeptablen Ungleichbehandlungen als unentbehrlich angesehen. [60]

[Rz 23] Sucht man nach einer Definition von «Rasse», stösst man auf mehrere ähnliche und auch mehr oder weniger umfangreiche, aber nicht übereinstimmende Umschreibungen: So z.B. als Gruppe von Menschen mit bestimmten

vererbbaren Merkmalen.[61] Oder: eine Gruppe von Menschen als Gesamtheit kollektiver Zuschreibung, die aufgrund besonderer physischer und/oder kultureller Eigenschaften von andern Gruppen verschieden sind und daher auch als minderwertig empfunden oder verstanden werden.[62] Oder: Eine Gruppe von Lebewesen mit bestimmten vererbbaren Merkmalen, wobei die Einschätzung der Gesellschaft den Ausgangspunkt des heute üblichen Verständnisses des Rassenbegriffs bilde, ein Obergebegriff auch für biologische Kategorien[63] (Hautfarbe, nationale Herkunft[64]) und ethnische Zugehörigkeit.[65] Ähnlich im Basler Kommentar: Bündel von mehr oder weniger äusserlich wahrnehmbaren Eigenschaften (Haut-, Augenfarbe, Physiognomie, Religion, Sprache), wie sie wahrgenommen werden (Fremdidentifizierung) oder sich selber identifizieren (Selbstidentifizierung).[66] Marcel Alexander Niggli verweist auf eine Klassifikation nach der Morphologie unter Einschluss der Verteilung von Gen-Häufigkeiten[67] und damit auf biologische Unterschiede, was sowohl aus biologischer und kulturanthropologischer Sicht gerade abgelehnt wird.[68]

[Rz 24] Eine sozial- oder kulturanthropologische Interpretation wird – soweit ersichtlich – in der rechtswissenschaftlichen Auslegung von «Rasse» nicht diskutiert, führte aber auch kaum zu mehr begrifflicher Stringenz. Das Bundesgericht verlässt sich auf den Duden.[69]

[Rz 25] Auffallend ist bei mehreren dieser Umschreibungen, dass die mit dem Ausdruck «Rasse» als anders Bezeichneten mehr oder weniger offen als «minderwertig» angesehen werden. Damit wird eine so umschriebene menschliche Eigenschaft selber direkt als etwas Minderwertiges gewertet, was dem Ziel der Rechtssetzung gerade diametral entgegenläuft. Das kann mit der nur negativen Konnotierung des Ausdrucks «Diskriminierung» ausschliesslich im Deutschen zusammenhängen (vorstehend, Rz. 4). Als objektive Umschreibung verschiedener Gruppen von Menschen kann dies nicht richtig sein. Es lässt aber auf die quasi inhärent vorhandene Meinung einer vermeintlichen Überlegenheit der Bezeichnenden (also bspw. «Weisse» gegenüber «Nichtweissen») schliessen.[70] Gerade die Feststellung «nicht weiss» zeigt bei Menschen, die aus Mischpartnerschaften stammen, die Absurdität von «Rasse» und «Ethnie» für deren «Kategorisierung» (vgl. Rz. 29). Freilich ist selbst diese unhaltbare Auffassung keineswegs mehr immer zutreffend: Im amerikanischen Wahlkampf hat sich gerade umgekehrt ein Minderwertigkeitsgefühl von «Weissen» gegenüber ihrem «schwarzen» Präsidenten und seiner Gattin manifestiert.[71] Und Weisse haben andere Weisse herabsetzend disqualifiziert («white trash»)[72].

[Rz 26] Nicht zu übersehen ist indessen v.a. die Ungenauigkeit und Ablehnung des Ausdrucks «Rasse» als rechtlicher Begriff.[73] Genau besehen, beruht die Feststellung, ob eine Diskriminierung aus Gründen (und nicht «wegen»[74]) der Rasse vorliege, nicht darauf, ob es Rassen als Menschenrassen gibt. Die Existenz verschiedener menschlicher Rassen wird naturwissenschaftlich und grundsätzlich auch rechtlich, wie vorstehend dargelegt, negiert. Trotzdem wird der Ausdruck in Art. 8 Abs. 2 BV verwendet. Somit geht es darum, ob das die Benachteiligung oder Fokussierung auslösende Merkmal sich als Teil einer landläufigen, aber unhaltbaren Rassenzuschreibung darstellt.[75] Daher kann «rassistische Diskriminierung» nur subjektiv unter Rückgriff auf (auch im Unterbewusstsein) bestehende Vorurteile oder als bewusste Schlechterbehandlung festgestellt werden.[76]

[Rz 27] Auch «Rasse» taugt, nach «Diskriminierung», somit als verfassungsrechtlicher hinreichend bestimmter Begriff nicht. Bisher stützt sich aber die Rechtswissenschaft hartnäckig durchwegs auf «Rasse» bzw. «Rassen», die es unter Menschen gerade nicht gibt, um darauf gestützt Ungleichbehandlungen just nach diesem nicht existierenden Anknüpfungsmerkmal als «Rassismus» zu bekämpfen.[77] Das ist unlogisch. Thornberry postuliert daher, es sei besser von ethnischen Gruppen zu sprechen.[78]

## 2. Zum Begriff der Ethnie

[Rz 28] «Ethnie» ist indessen keineswegs präziser als «Rasse» - aber damit verbunden.[79] Es handle sich um einen schwer fassbaren kultur- bzw. sozialanthropologischen Begriff.[80] Er liegt im Schnittstellenbereich zwischen naturwissenschaftlicher[81] und philosophischer Anthropologie, Rechtsphilosophie und Ethik. In der Kulturanthropologie wird «Ethnie» in eine Praxis- und eine Forschungskategorie unterteilt.[82] Das führt zu einer subjektiven und einer objektiven Auslegung von «ethnischer Herkunft». Aber auch diese Unterscheidung bleibt in diesem Zusammenhang unscharf: objektiv kann «Ethnie» nur eine Kategorie der Wissenschaft sein. Subjektiv bezieht sich «Ethnie» auf die Selbst- und die Fremdwahrnehmung, was zu unterschiedlichen Ergebnissen führen kann.[83] Subjektive Wahrnehmung beruht relational auf der Unterscheidung zwischen sich selbst und einer anderen Person nach individuellen Kriterien-Parametern[84] und bestimmt somit das «Fremdsein» von sich selber oder der anderen Person(en), je nach Ort des Geschehens bzw. der lokalen Mehrheit. Woraus ergibt sich aber der Parameter, bspw. um sich nicht (als Teil einer angenommenen Mehrheit oder Minderheit) selber auszuschliessen? Dies «Bestimmung» folgt der überindividuellen Einordnung von Merkmalen, wie sie gemeinhin bzw. landläufig[85] oder nach dem «gesunden Menschenverstand» (common sense[86]) wahrgenommen werden. In der heutigen stark pluralistischen Gesellschaft mit rasch wechselnden «main stream»-Auffassungen oder solchen der politischen Korrektheit beruht die durch «landläufig» oder ähnlich vage Ausdrücke geprägte «Bestimmung» auf einer wackligen Grundlage. Der Rückgriff ausschliesslich auf Anleihen kulturanthropologischer und damit weitgehend diskurstheoretischer Ansätze zu Begriffsinhalten ist für die Rechtsetzung aber ebenso problematisch, da damit die geforderte rechtsstaatliche Bestimmtheit nicht zu erzielen ist,[87] was insbesondere, freilich nicht nur, für Strafrechtstatbestände gilt. Nicht eindeutig festgelegte Begriffe werden bei sprachlich-grammatikalischer und insbesondere teleologischer Auslegung[88] und Sprachlogik für die Ermittlung des Sinns so mehr zur Rechtserfindung als zur Rechtsfindung.[89]

## 3. Zum Begriff der «Hautfarbe»

[Rz 29] Die Hautfarbe ist eines dieser äusserlichen Merkmale. Genannt wird sie als Anknüpfungskriterium für ein allgemeines Diskriminierungsverbot im 12. ZP zur EMRK.[90] Auch wenn es Menschen mit offensichtlich deutlich unterschiedlichen Hautfarben gibt, ist die Hautfarbe kein zuverlässiges Kriterium, was sich schon an Personen von Eltern, die selber verschiedener Hautfarbe sind, zeigt.[91] In Europa und den USA dürfte es auch nicht um die Hautfarbe an sich gehen, sondern um «nicht ganz weiss»[92] als vermeintliches Merkmal der Andersartigkeit oder des «Fremden» für alle anderen. Anders als «Rasse» ist die Hautfarbe indessen eine vererbte äusserlich (mehr oder weniger deutlich) wahrnehmbare Eigenschaft, ein Faktum. Aber dieses äusserlich Wahrnehmbare lässt keine Schlüsse auf den Ort der Geburt (auch ein Kriterium der Herkunft), v.a. aber nicht auf das innere Wesen eines Menschen, seine Erziehung, Sprache, Bildung, Kultur, seine Integration in einer «andersfarbigen» Mehrheit, auf sein «Sein» zu. Hautfarben sind als Anknüpfungskriterium daher ungeeignet für die Begründung von Andersartigkeit oder Fremdheit. Damit wird wiederum die subjektive Fokussierung auf eine Person selber konstitutiv zur Begründung der äusserlichen Andersartigkeit der andern, was mit deren tatsächlichem «So-Sein» überhaupt nicht übereinstimmen muss.[93]

## 4. Die in der BV ausgedrückten Anknüpfungskriterien

[Rz 30] In Art. 8 Abs. 2 BV werden im hier interessierenden Kontext explizit die Ausdrücke «Rasse» und «Sprache» (im Zusammenhang mit ethnischer Herkunft) genannt, nicht aber die Hautfarbe. Das Diskriminierungsverbot ist jedoch weiter gefasst, da die Aufzählung durch das «namentlich» nicht abschliessend zu verstehen ist.[94]

### a) «Rasse»

[Rz 31] Das mit der expliziten Verwendung in Art. 8 Abs. 2 Verfassungsrecht gewordene Anknüpfungskriterium wird in der Botschaft über eine neue Bundesverfassung nicht definiert.[95] Hingegen findet sich in der Botschaft zur ARK[96] eine

nicht widerspruchsfreie Umschreibung: «Rasse» ebenso wie «Hautfarbe» seien biologische und physische Merkmale; der Begriff der Rasse schliesse subjektive und soziale Komponenten ein. «Eine Rasse ist in diesem breiten – soziologischen – Sinn eine Menschengruppe, die sich selbst als unterschiedlich von andern Menschengruppen versteht und/oder so verstanden wird, auf der Grundlage angeborener und unveränderlicher Merkmale». [97] Ob aus dem Stillschweigen in der Botschaft zum VE 96 der BV über den Begriff der «Rasse» in Art. 8 Abs. 2 angenommen werden soll, die Umschreibung aus der Botschaft zur ARK sei nach wie vor massgebend, darf aufgrund der seitherigen rechts- und sozialwissenschaftlichen Erkenntnisse bezweifelt werden.

### b) «Ethnie»

[Rz 32] «Ethnie» kommt in Art. 8 Abs. 2 BV nicht vor, wohl aber «Herkunft». Aber auch «Herkunft» wird in der Botschaft über eine neue Bundesverfassung nicht definiert. Das Wort kommt nur als Klammerausdruck (mit «Rasse») vor. [98] Die in der Botschaft zur ARK für «Rasse» verwendete Umschreibung trifft jedoch eher auf die (ethnische) Herkunft zu. [99]

### c) «Hautfarbe»

[Rz 33] Die Hautfarbe wird in Art. 8 Abs. 2 BV nicht ausdrücklich als Anknüpfungskriterium verwendet. Demzufolge erscheint der Ausdruck auch nicht in der Botschaft zur neuen BV. In derjenigen zur ARK indessen wird die Hautfarbe zusammen mit der «Rasse» als biologisches und physisches Merkmal bezeichnet. [100] Zusätzlich wird vermerkt, die Hautfarbe gehöre zu den Merkmalen der Rasse. [101] Mindestens systematisch gesehen, ist diese Ergänzung fragwürdig und steht im Gegensatz zu den Erkenntnissen der naturwissenschaftlichen und kulturanthropologischen Forschung.

## 5. Die in den Kantonsverfassungen ausgedrückten Anknüpfungskriterien

[Rz 34] Die Kantonsverfassungen präsentieren sich hinsichtlich der Anknüpfungsmerkmale, die im vorliegenden Zusammenhang interessieren, sehr unterschiedlich.

[Rz 35] Zwei Verfassungen enthalten keine Bestimmung betreffend Diskriminierungsverbot und verweisen auch nicht auf die BV bzw. deren Grundrechtskatalog (oder Art. 8 Abs. 2 BV im Speziellen). [102] Eine zweite Gruppe von Kantonsverfassungen verweist ausschliesslich auf die BV [103] sowie auch auf die massgebenden völkerrechtlichen Verpflichtungen. [104] Eine dritte Gruppe enthält ohne Anknüpfungskriterien ein generelles Diskriminierungsverbot (z.B. «Niemand darf diskriminiert werden.»). [105] In den Kantonsverfassungen, welche die hier interessierende Anknüpfungsmerkmale enthalten, finden sich nachfolgend aufgeführte Auflistungen, wobei einige durch «namentlich» oder «insbesondere» den nicht abschliessenden Charakter der Anknüpfungsmerkmale feststellen.

| Kanton | nicht abschlies-send | Rasse | Herkunft | Abstammung | Ethnie / ethnisch | Genetische Merkmale | Sprache | Hautfarbe |
|---|---|---|---|---|---|---|---|---|
| ZH, Art. 11 Abs. 2 | x | x | x | | | x | x | |
| BE, Art. 10 Abs. 1 | x | x | x | | | | x | x |
| UR, Art. 11 Abs. 2 | | x | x | | | | x | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| NW Art. 2 Abs. 2 | | x | x | | | | x | |
| GL, Art. 4 Abs. 2 | | | x | | | | x | |
| BS, § 8 Abs. 2 | x | x | x | | x | x | x | |
| BL, § 7 Abs. 2 | x | | x | x | | | | |
| AR, Art. 5 Abs. 2 | x | x | x | | | | x | x |
| AG, § 10 Abs. 2 | | x | x | x | | | x | |
| TI, Art. 7 Abs. 1 | | x | x | | | | | |
| VD, 10 Abs. 2 | x | | x | | | x | x | (Aussehen) |
| GE, Art. 15 Abs. 2 | x | | x | | | | | |
| JU, Art. 6 Abs. 2 | | x | x | | | | | |

[Rz 36] Im Zuge der Totalrevision der Kantonsverfassung Basel-Stadt verwies die Spezialkommission Grundrechte auf Fortschritte der Bio-Wissenschaft, damit der genetischen Forschung, und postulierte den Einbezug des «Diskriminierungstatbestandes» der «genetischen Merkmale».[106] Sie bezog sich auch auf Art. 11 des Übereinkommens über Menschenrechte und Biomedizin.[107] Wiewohl sich dieses Verbot auf medizinische Zusammenhänge sowie deren allfällige Konsequenzen bspw. im Versicherungswesen bezieht,[108] weist die Formulierung «jede Diskriminierung…» auf eine umfassendere Anwendbarkeit dieses Merkmals hin, sofern dessen Erkennbarkeit (Evidenz) und Relevanz (in der parallelen Laiensphäre[109]) in einem konkreten Fall massgebend ist.

[Rz 37] Die Vielzahl der Varianten deutet auf die Unsicherheit der (Verfassungs-) Gesetzgebung hin, wie, d.h. nach welchen Kriterien, Diskriminierung am besten bekämpft werden kann. Entsprechend schwierig ist es, in nicht eindeutig klaren Fällen, bspw. durch die Art der herabwürdigenden Behandlung, auf deren diskriminierenden Charakter zu schliessen (vgl. nachfolgend V.).

## 6. Die Polizeigesetze der Kantone hinsichtlich dieser Begriffe

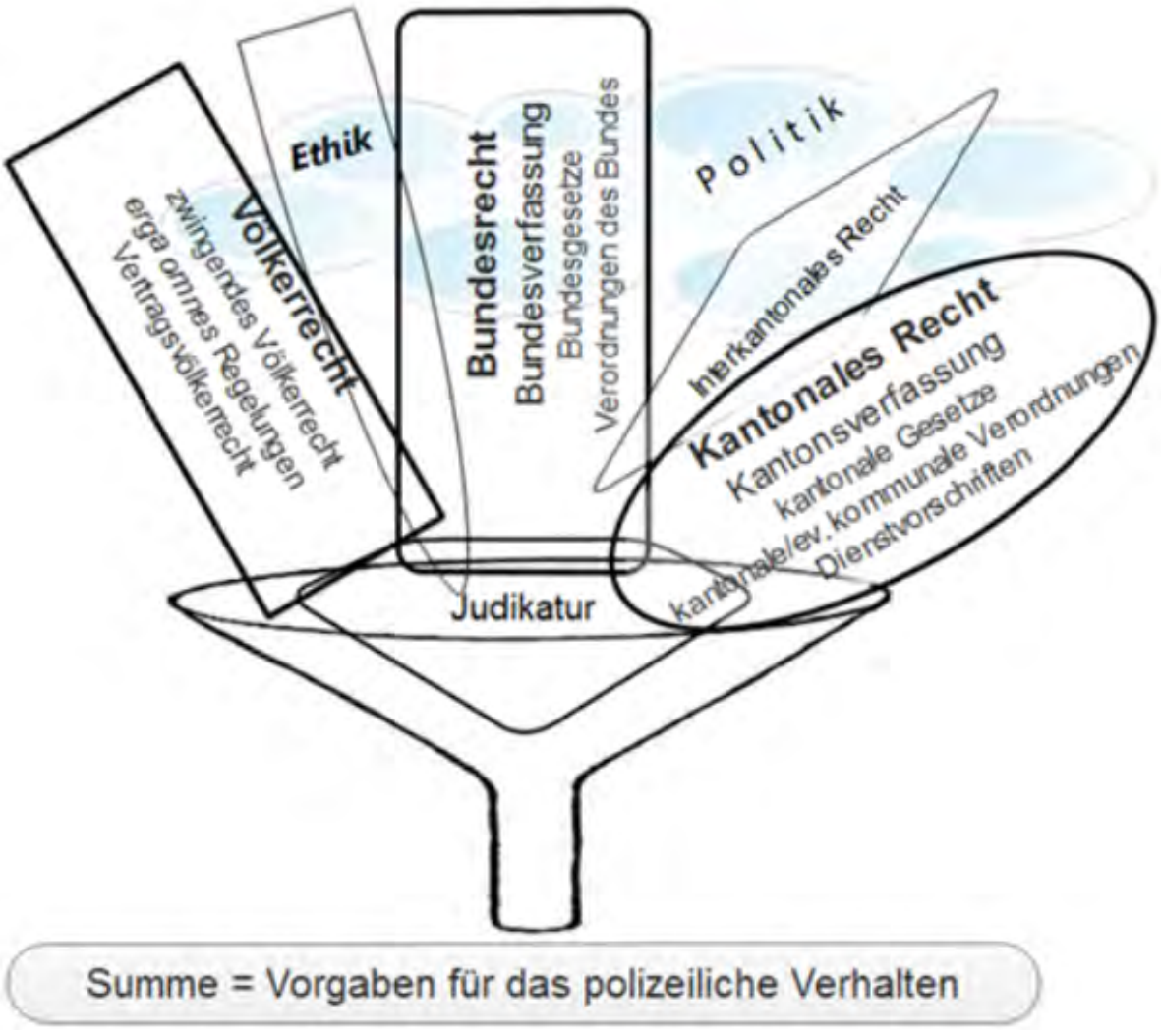
[Rz 38] In keinem der kantonalen Polizeigesetze kommen die hier relevierten Ausdrücke vor. Da auch «Diskriminierung» oder «diskriminieren» mit Ausnahme von Basel-Stadt und Jura (in anderer Formulierung) nicht zu finden sind, kann festgehalten werden, dass die Polizeigesetze diese besondere Problematik nicht spezifisch regeln.

[Rz 39] Andererseits verweist der überwiegende Teil[110] der Polizeigesetze auf die übergeordnete Rechtsordnung[111] des Bundes und ihre Kantons. Die meisten erwähnen ausdrücklich das Gesetzmässigkeitsprinzip[112], das sich auch auf die Vorgaben der BV bezieht.

## III. Der Rechtsrahmen für Personenkontrollen insgesamt

### 1. Generell

[Rz 40] Das Polizeirecht ist ein dichtes Gewebe aus den ratifizierten massgebenden weltweit gespannten völkerrechtlichen Abkommen[113] und aus bilateralen Verträgen betr. Zusammenarbeit der Polizeibehörden,[114] den übernommenen Konventionen des Europarates,[115] dem EU-Recht qua Schengen-[116] und Dublin-Assoziierungsabkommen,[117] dem Bundes-, dem überordneten kantonalen, dem interkantonalen Recht sowie der eigenen Polizeigesetzgebung.[118] Dabei sind ethische Forderungen von grosser Bedeutung.[119] Und massgebend ist selbstverständlich die Judikatur in der Auslegung dieser Rechtsgrundlagen.[120]




[Rz 41] In diesem überaus dichten polizeirechtlichen Gewebe sind auch die Grundlagen und die Schranken für Personenkontrollen enthalten.

[Rz 42] Personenkontrollen, d.h. ausschliessliche Identitätsfeststellungen, berühren die persönliche Freiheit (Art. 10 Abs. 2 BV, Art. 8 Abs. 1 EMRK), wenn auch nur leichtem Ausmass.[121] Sie bedürfen daher nach Art. 36 Abs. 1 BV einer

gesetzlichen Grundlage.[122] Personenkontrollen sind in allen kantonalen Polizeigesetzen geregelt: Die Polizei erhält dadurch die Befugnis, zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung[123] Personen anzuhalten und ihre Identität zu überprüfen.[124] Umgekehrt sind die Personen, die von der Polizei kontrolliert werden, verpflichtet, Angaben über ihre Identität zu machen.[125] Voraussetzung ist ein dafür hinreichender Grund, also die begründbare Annahme, die betroffene Person sei zur Fahndung ausgeschrieben, sei illegal eingereist oder halte sich illegal in der Schweiz auf oder ein plausibler minimaler Anfangsverdacht auf eine Widerhandlung.[126] Die Personenkontrolle muss im Einzelfall notwendig, im öffentlichen Interesse und verhältnismässig sein, um solche Aufgaben zu erfüllen.[127] Anders ausgedrückt: Identitätsüberprüfungen dürfen nicht anlassfrei[128] bzw. voraussetzungslos[129] vorgenommen werden.

### 2. Aspekte des Rechts der öffentlichen Sicherheit und Ordnung

[Rz 43] Die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, die Gefahrenabwehr, die Durchsetzung der Rechtsordnung, ist eine Pflicht u.a. der Polizei. Diese fliesst aus dem (aktiven) Legalitätsprinzip.[130] Es ist ihr nicht anheimgestellt, ob sie aus «Opportunitätsgründen» die Befolgung von Gesetzen, die in ihren Zuständigkeitsbereich fallen, durchzusetzen bzw. Gefahren abzuwehren sucht oder nicht. Dazu gehören auch einzelgesetzliche Aufgaben wie bspw. der Vollzug des Bundesgesetzes über die Ausländerinnen und Ausländer[131] oder des Bundesgesetzes über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen.[132] Der UNO Menschenrechtsausschuss hat in einem Entscheid 2009 festgestellt, dass Identitätskontrollen zur Bekämpfung der illegalen Einwanderung einer legitimen Zielsetzung dienten.[133] Einschränkungen von diesem Grundsatz ergeben sich im Rahmen des Verhältnismässigkeitsprinzips[134] und des engen Entschliessungs- oder Einzelfallermessens.[135] Dieses Entschliessungsermessen seinerseits ist – nach den zulässigen Kriterien von Auffälligkeiten hinsichtlich von Personen, Örtlichkeiten oder Umständen[136] – geprägt davon, was als genügender Anfangsverdacht (reasonable suspicion)[137] gilt (Näheres dazu nachfolgend, Rz. 46 ff., 53).

### 3. In Bezug auf «Rasse», «Ethnie» und «Hautfarbe»

[Rz 44] Aus dem Diskriminierungsverbot gemäss den hier relevierten Anknüpfungskriterien ergibt sich, dass weder «Rasse» noch «ethnische Herkunft» oder die Hautfarbe allein hinreichender Grund für eine Personenkontrolle sein können.[138]

## IV. Abgrenzungskriterien zwischen erlaubter und diskriminierender Personenkontrolle

### 1. Grundsätzlich

[Rz 45] Nach dem materiellen Verständnis des Diskriminierungsbegriffs[139] sei das verpönte Ergebnis einer Behandlung und nicht die Behandlung selber massgebend. Dies bedeutet vom theoretischen Ansatz her ein Wandel: Die «Rasse», quasi als Objekt, als Eigenheit des Rechtssubjekts, der Einschätzung oder Behandlung, wird durch die Behandlung selber als moralisch nicht erwünscht bzw. ethisch verwerflich resp. durch deren Ergebnis ersetzt. Damit bleibt zu umschreiben, was genau ein verpöntes Ergebnis ist und wer dies worauf gestützt feststellt. Materiell geht es bei der rechtsungleichen Behandlung, wie erwähnt, um eine Beeinträchtigung der Menschenwürde einer Person, ihre Herabwürdigung, allein auf Grund ihrer «Rasse», «ethnischen Herkunft» oder Hautfarbe.[140] Wie auch bereits vermerkt, müssen Wertschätzung und Menschenwürde nicht identisch sein. In einem Urteil von 2001 hält das Bundesgericht fest: «Die Menschenwürde betrifft das letztlich nicht fassbare Eigentliche des Menschen und der Menschen und ist unter Mitbeachtung kollektiver Anschauungen ausgerichtet auf Anerkennung des Einzelnen in seiner eigenen Werthaftigkeit und individuellen Einzig- und allfälligen Andersartigkeit».[141] Menschenwürde entziehe sich in der Offenheit ihrer Erscheinungsformen einer abschliessenden positiven Festlegung; sie realisiere sich in

menschlichen Akten der Anerkennung oder werde vernichtet in Erniedrigung und Demütigung.[142] Darin liegt von der handelnden (oder unterlassenden) Person her notwendigerweise eine subjektiv geprägte negative Haltung oder zumindest eine individuelle negative Einschätzung (selbst ohne eine generell negativ geprägte Haltung) der andern Person gegenüber. Diese ist aber nicht notwendigerweise mit «Rasse» verknüpft.

[Rz 46] Keiner Diskussion bedürfen Verhaltensweisen von Polizeiangehörigen, bei denen eine negative innere Haltung gegenüber kontrollierten Personen offenkundig wird. Sie stellen zweifelsfrei Diskriminierungen im Sinne von Art. 8 Abs. 2 BV dar. Dazu zählen ebenso allfällige Personenkontrollen, welche ausschliesslich auf äusserliche Merkmale abstellen; dies entspricht dem verpönten racial profiling[143], sofern die auslösenden Eigenschaften eines Menschen damit in Verbindung zu bringen sind. Nach rechtlichen Kriterien schwierig – und im Ergebnis wohl überwiegend kontrovers bleibend – zu beurteilen sind Fälle, in denen sich Polizeiangehörige weder von einer negativen Haltung noch einem unbewussten (negativen) Vorurteil gesteuert zu einer Personenkontrolle entschliessen, da sie zusätzlich zu äusseren Erkennungsmerkmalen bei einer Person ein Verhalten erkennen oder zu erkennen vermeinen, das bei ihnen einen plausiblen Verdacht hinsichtlich einer Rechtswidrigkeit aufkommen lässt. Die kritische Schwelle liegt somit in der Frage, was in einem Einzelfall als Plausibilität einer («vernünftigen») Verdachtsbegründung genügt.[144] Dabei sind auch Örtlichkeiten und Umstände von Belang.

[Rz 47] Der englische Code A des UK Home Office betr. Powers of Stop and Search[145] nennt drei verschiedene Gehalte, die für die Annahme von vernünftigen Gründen für einen Verdacht («reasonable grounds for suspicion») gelten:

- Verdachtsgründe gestützt auf Informationen und/oder die Nachrichtenlage[146]
- Verdachtsgründe gestützt auf die Zugehörigkeit zu bestimmten Gruppen[147]
- Verdachtsgründe ohne spezifische Information oder entsprechende Nachrichtenlage gestützt auf das Verhalten einer Person.[148]

[Rz 48] Eine genauere Betrachtung dieser im Weiteren noch detaillierter ausgeführten Kodex-Vorschriften ergibt, dass die erst Gruppe von Verdachtselementen, sofern sorgfältig erwogen, auch hierzulande keine Annahme für eine Diskriminierung liefert. Die Zugehörigkeit zu einer bestimmten Gruppe (2. Fallgruppe) kann in der Schweiz in dieser Formulierung jedoch nicht in jedem Fall für eine Personenkontrolle genügen. Die Umschreibung für die rechtmässige Annahme eines vernünftigen Verdachts ohne spezifische Informationen (3.Gruppe) vermag auch nicht mehr beizutragen als was das Bundesgericht bisher für Personenkontrollen generell fordert. Damit bleibt die Differenz zwischen dem für eine Diskriminierung allein als konstitutiv betrachteten Ergebnis (aus der Sicht der betroffenen Person oder rein theoretischer Betrachtungswiesen)[149] und dem Motiv für eine Personenkontrolle, der Plausibilität für die Annahme eines «vernünftigen Verdachts», ungelöst.

[Rz 49] Diese Problematik zeigt sich vorallem, jedoch nicht nur, hinsichtlich von Personenkontrollen, die zur Überprüfung der Rechtmässigkeit der Einreise (unter dem Regime des Verbotes systematischer polizeilicher Kontrollen an den Binnengrenzen)[150] oder des legalen Aufenthaltes durchgeführt werden. Dieses genügende Mass an Plausibilität für die Annahme eines «vernünftigen Verdachts» wird, bei allen Anstrengungen, es bei allen Personenkontrollen von Anfang an zu erreichen, im Streitfall letztlich nur eine unabhängige Instanz bzw. ein Gericht im Einzelfall feststellen können. Dies zeigt sich am Beispiel, das dem Urteil des Bezirksgerichts Zürich vom 7. November 2016 zugrunde liegt (dazu nachfolgend, V, Rz. 57).

## 2. Alltagssituationen

[Rz 50] Es dürfte sich bei den Alltagssituationen um vier Stereotype handeln: (a) Kontrollen im Grenzraum oder in (Grenz-)Bahnhöfen, (b) Kontrolle auf Grund eines Signalements einer Person, nach der im Zusammenhang mit einem

Delikt gefahndet wird, (c) Kontrollen in einer Umgebung mit überdurchschnittlicher Kriminalität mit notorisch überdurchschnittlich hohem Anteil Verdächtiger bestimmter Herkunft gegenüber gewissen Vergleichszahlen sowie (d) Kontrollen von ihrem Aussehen nach «fremden» Personen, die sich beim Erscheinen der Polizei unversehens erkennbar anders, auffällig, verhalten, um – nach Auffassung der Polizeiangehörigen –dadurch nach Möglichkeit einer Kontrolle zu entgehen.

a. Die illegale Einreise ist nicht gestattet, strafbar[151] und nach Möglichkeit zu verhindern.[152] In diesem Zusammenhang hat der UNO Menschenrechtsausschuss[153] die bereits erwähnte, mehrfach interessante Entscheidung getroffen: «The Committee considers that identity checks carried out … to control illegal immigration, serve a legitimate purpose. However, when the authorities carry out such checks, the physical or ethnic characteristics of the persons subjected thereto should not by themselves be deemed indicative of their possible illegal presence in the country. Nor should they be carried out in such a way as to target only persons with specific physical or ethnic characteristics».[154] Zum einen wird festgehalten, dass die Kontrolle (bzw. Verhinderung) der illegalen Einreise ein legitimes Ziel sei. Dann wird eingeschränkt, dass physische oder ethnische Charakteristika für sich allein genommen nicht ausschlaggebend sein sollen. Nicht gesagt wird jedoch, wie denn bspw. im Grenzraum die (zeitweise sehr starke) illegale Einwanderung von Menschen bspw. (angenommener) afrikanischer Herkunft effektiv kontrolliert werden kann, ohne gegen das Diskriminierungsverbot zu verstossen. Zu erinnern ist in diesem Zusammenhang für den Schengen-Raum daran, dass systematische Grenzübertrittskontrollen (die einen Bezug auf «physische oder ethnische Charakteristika» ausschlössen) an den Binnengrenzen ebenso wie Kontrollen im Raum der Binnengrenzen, die solchen nahekommen, nicht gestattet sind.[155] Nach der einen Vorschrift sollen illegale Einreisen verhindert werden, nach einer zweiten dürfen keine systematischen Grenzkontrollen durchgeführt werden, denen alle unterzogen werden, und nach einer dritten Rechtsquelle dürfen physische oder ethnische Merkmale, die z.B. bei der derzeitigen Migrationsstärke objektiv auf illegale Grenzübertritte hindeuten, nicht zum Anlass von Kontrollen genommen werden. Das kommt in der Praxis der Quadratur des Kreises gleich. Dies ergibt sich zudem aus einer Formulierung des Bundgerichts hinsichtlich der Notwendigkeit einer Personenkontrolle zur polizeilichen Aufgabenerfüllung: «Mit dem Begriff der Notwendigkeit wird zum Ausdruck gebracht, dass spezifische Umstände vorliegen müssen, damit die Polizeiorgane Identitätskontrollen vornehmen dürfen, dass die Kontrolle nicht anlassfrei erfolgen darf. Erforderlich können solche etwa sein, wenn sich Auffälligkeiten hinsichtlich von Personen, Örtlichkeiten oder Umständen ergeben und ein entsprechendes polizeiliches Handel gebieten».[156] Bedeutet nach Bundesgericht eine Auffälligkeit hinsichtlich von Personen im Zusammenhang mit Örtlichkeit somit einen eine Kontrolle legitimierenden Anlass, scheint das gemäss dem zitierten Entscheid des Menschenrechtsausschusses gerade nicht der Fall zu sein.
b. Personenbeschreibungen (Signalemente) in Fahndungsdatenbanken beziehen sich neben den Personalien, sofern bekannt, auf die äussere Erscheinung. Darin sind physische Merkmale enthalten, die auch auf die «ethnische Herkunft» Rückschlüsse erlauben, sofern zutreffend. Nicht zuzustimmen ist daher der Feststellung, «ein Sonderproblem stell(e) sich bei rassenspezifischen Täterbeschreibungen: So kann es zulässig erscheinen, dass die Polizei nur nach einem Täter dunkler Hautfarbe sucht, wenn beispielsweise alle verfügbaren Zeugen eine entsprechende Beschreibung des Täters abgegeben haben und keine widersprechenden Hinweise vorliegen».[157] Dies führte, in Kenntnis der notorischen Unterschiede in Aussagen von Augenzeugen, zu einer mindesten mittelbaren Besserbehandlung bzw. positiven Diskriminierung allfälliger Verdächtiger mit Merkmalen, die auf eine andere «ethnische Herkunft» schliessen liessen. Dies widerspräche kriminalistischen Grundregeln (Signalementslehre[158]) fern eines «racial profiling» und wäre auch nicht umsetzbar, wenn bspw. nur das Opfer Aussagen machen kann.
c. Als Kriterium für diskriminierende Personenkontrollen werden oft statistische Vergleichszahlen verwendet.[159] Auch beim Beizug von Statistiken ist Vorsicht geboten. Wiewohl im Handbuch «Diskriminierendes Profiling» darauf hingewiesen wird, die Ergebnisse der EU-MIDIS Studie könnten nicht als endgültiger Beweis dafür angesehen werden, dass es bei der Polizei Praktiken mit diskriminierendem Ethnic Profiling gebe,[160] wird als

Indikator für diskriminierende Personenkontrollen das Verhältnis der Zahl der kontrollierten Personen einer bestimmten Gruppe zur entsprechenden Wohnbevölkerung als Anteil an der Gesamtbevölkerung zugezogen.[161] Dieses Verhältnis muss jedoch keineswegs aussagekräftig sein, zumindest nicht in Grenzräumen. So zeigt bspw. die Kriminalstatistik des Kantons Basel-Stadt, dass von den in der Betäubungsmitteldelinquenz identifizierten und ermittelten Verdächtigen der Anteil der Ausländer, die weder zur Wohnbevölkerung noch zur Asylgruppe gehören, gleich gross oder grösser ist als die entsprechende Wohnbevölkerung.[162] Noch deutlicher ist diese Ungleichheit qua Betäubungsmittelhandel von beschuldigten Ausländern mit Wohnort Schweiz zu den «übrigen Ausländern» auf gesamtschweizerischer Ebene: Die absolute Zahl der «übrigen Ausländer» ist mehr als doppelt so hoch wie diejenige der hier wohnenden beschuldigten Ausländer (einschliesslich solche im Asylverfahren).[163] Das lässt auf einen grossen Anteil von «Kriminaltouristen» oder sich illegal in der Schweiz aufhaltender Verdächtiger schliessen.

d. Die «Trefferquote»[164] ist ebenso nicht notwendigerweise ein Beleg für diskriminierende Personenkontrollen: die Trefferquote hinsichtlich Verletzung des Ausländergesetzes bei den Ausländern, die nicht zur Wohnbevölkerung und nicht zur Asylgruppe gehören, beträgt 78%.[165]
e. Auch die vierte Konstellation, in der diskriminierendes Verhalten der Kontrollierenden vermutet wird, stellt keine unterschiedliche Behandlung gegenüber Personen, welche nach den hier interessierenden Anknüpfungskriterien «fremd» sind, dar: Verhält sich jemand beim Gewahrwerden von Polizeiangehörigen in dem Sinne auffällig, sich einer Kontrolle entziehen zu wollen, führt ein solches Verhalten ohne Ansehen der Person oft zu einer Kontrolle. Die Personenkontrolle wird in einer solchen Situation nicht auf «allein auf Grund ihrer Zugehörigkeit zu einer bestimmten Gruppe»[166] durchgeführt, sondern mit einem sachlichen Kriterium verknüpft,[167] weshalb es sich nicht um eine Diskriminierung handeln muss.

## 3. Indirekte Diskriminierung

[Rz 51] Ein Wort zur Umschreibung einer indirekten Diskriminierung: Im Handbuch der Europäischen Agentur für Grundrechte findet sich unter «indirekte Diskriminierung» «im Kontext des Ethnic Profiling» folgendes Beispiel: «Anhalten jedes zehnten Fahrzeugs in der Stadt X in der Zeit zwischen 21:00 und 01:00 Uhr)», da dies negative Auswirkungen auf eine bestimmte Bevölkerungsgruppe haben könne, die dann vermehrt unterwegs sei.[168] Just das Kriterium einer rein numerischen Auswahl der zu Kontrollierenden kann Basis weder einer direkten noch einer indirekten Diskriminierung bilden. Die Kontrolle dient der Entdeckung und Verhinderung unterschiedlicher Delikte, ohne jeden Bezug zur allfälligen Gruppenzugehörigkeit nach den in Frage stehenden Anknüpfungskriterien.[169] Der Verzicht auf eine derart angeordnete Verkehrskontrolle bedeutete mit dieser Argumentation umgekehrt eine ungerechtfertigte Bevorzugung so definierter Bevölkerungsteile zu Lasten der Verkehrssicherheit.

[Rz 52] Schliesslich fällt eine Aussage des inzwischen abgetretenen Vorsitzenden der Europäischen Agentur für Menschenrechte, Morten Kjaerum, auf: Er erklärte als Warnung vor «ethnischem Profiling»: «National plans, backed by the European Commission, to confiscate the travel documents of people leaving to fight in Iraq or Syria could have the same result. Policies, he says, need to be designed with fundamental rights from the outset».[170] Das ist, mit Verlaub, Unsinn, denn die Selektion erfolgt aufgrund der mit hoher Wahrscheinlichkeit anzunehmenden Unterstützung einer terroristischen Organisation oder der Beteiligung an schwerwiegenden Verbrechen und nicht der Religion, die – u.a. von einigen Leuten, welche in Irak oder Syrien kämpfen wollen – als Konvertiten erst gerade angenommen worden ist. Daher entfällt in solchen Fällen auch das Kriterium des «wesentlichen und nicht oder nur schwer aufgebbaren Bestandteil(s) der Identität der betreffenden Person». Schwer aufgebbar ist dieser Bestandteil der Identität offensichtlich nicht – und auch wieder umkehrbar. Es kann ja wohl auch nicht sein, dass Personen wegen ihrer Zugehörigkeit zu einer Religion unbehelligt gelassen werden, wenn konkrete Indizien vorliegen, dass sie schwere Verbrechen zu begehen beabsichtigen oder nach solchen Verhaltensweisen aus entsprechenden Ländern zurückkehren.

### 5. Zwischenergebnis

[Rz 53] Nach der hier vertretenen Auffassung rechtlich zulässig sind demnach Kontrollen von Personen, die sich durch äusserlich erkennbare Merkmale (v.a. Hautfarbe, Physiognomie bzw. nach einem dieser Anknüpfungskriterien) unterscheiden, sofern die Polizeiangehörigen die zu kontrollierenden Personen von ihrer inneren Haltung her oder aus (auch un-) bewusster Voreingenommenheit wegen ihrer (vermeintlichen) «Andersartigkeit» nicht als minderwertig betrachten, sie in ihrer Würde also nicht herabsetzen, sondern, ihre Identität ohne Ansehen der Person [171] – gestützt auf einen plausiblen, d.h. durch objektive Dritte nachvollziehbaren Sicht, vernünftigen Anfangsverdacht für eine Rechtswidrigkeit überprüfen. [172] Voraussetzung ist dabei, dass sie ein gewichtiges und legitimes öffentliches Interesse verfolgen, als geeignet und erforderlich betrachtet werden können und sich gesamthaft als verhältnismässig erweisen. [173]

[Rz 54] Diskriminierend sind umgekehrt Personenkontrollen, wenn die Kontrollierenden durch ihre innere Haltung oder auch unbewusste Vorurteile eine Person allein aus Gründen ihrer (vermeintlichen) «Andersartigkeit» als minderwertig betrachten und/oder ausgrenzen wollen, mithin die negative Haltung Kontrollmotiv ist, die polizeilichen Gründe (selbst durch eine innere Selbsttäuschung) nur vorgeschoben [174] sind oder es dem Anfangsverdacht auf eine Rechtswidrigkeit an Plausibilität mangelt. [175] Dieser Mangel an Plausibilität kann als Indiz einer negativen Einstellung oder einer unbewussten Vorurteilsbelastung herangezogen werden.

## V. Zur Frage der Nichtigkeit von Personenkontrollen

[Rz 55] Damit stellt sich die Frage, wie der einer Personenkontrolle allenfalls anhaftende Mangel hinsichtlich seiner Schwere und den sich daraus ergebenden Folgen zu gewichten ist. Nach konstanter bundesgerichtlicher Rechtsprechung ist, gestützt auf die Evidenztheorie, eine Entscheidung nichtig, «wenn der ihnen anhaftende Mangel besonders schwer ist, wenn er sich als offensichtlich oder zumindest leicht erkennbar erweist und die Rechtssicherheit durch die Annahme der Nichtigkeit nicht ernsthaft gefährdet wird». Inhaltliche Mängel einer Entscheidung führten nur ausnahmsweise zur Nichtigkeit. [176] Als besonders schwer gilt etwa ein offensichtlicher Verstoss gegen die Bundesverfassung. [177] Das ist zwar für Rechtsakte dogmatisch entwickelt, aber ohne Weiteres auch auf intervenierende Realakte übertragbar. Ergänzend stellte das Bundesgericht fest, Nichtigkeit könne «beispielsweise in der fehlenden gesetzlichen Grundlage für den Erlass des Entscheides liegen». [178] Ebensowenig gelten nach Bundesgericht «andere nichtige Motive» als Rechtsgrundlage für eine Identifikation. [179] Dabei wird auf den Leitentscheid aus dem Jahr 1983 verwiesen, wonach Identitätsüberprüfungen keinen «caractère vexatoire ou tracassier» haben dürfen. [180] «Vexatoire» bedeutet demütigend, kränkend, «tracassier» schikanös. Daraus ergibt sich zwangslos, dass Personenkontrollen, die offenkundig oder leicht erkennbar ausschliesslich auf äusserlich erkennbare Merkmale gestützt werden, als nichtige Realakte zu beurteilen sind. [181] Ist die Offenkundigkeit oder leichte Erkennbarkeit der Abstützung einer Personenkontrolle ausschliesslich auf erkennbare äusserliche Merkmale nicht gegeben, ist diese anfechtbar.

[Rz 56] Im vorliegenden Zusammenhang ergibt sich aus dem dritten Kriterium der Evidenztheorie, wonach die Rechtssicherheit durch die Annahme der Nichtigkeit nicht ernsthaft gefährdet werden dürfe, ein Paradoxon: Die Nichtigkeit einer offenkundig oder leicht erkennbar ausschliesslich auf äusserliche Merkmale abgestützten Personenkontrolle gefährdet die Rechtssicherheit gerade nicht, sondern verhilft ihr in solchen Fällen umgekehrt zum Durchbruch. Just aus diesem Grund allein durfte die Indentitätsüberprüfung nicht durchgeführt oder deren Nichtigkeit muss hinterher von sämtlichen rechtsanwendenden Behörden von Amtes wegen festgestellt werden. [182]

[Rz 57] Dieser Rechtsfrage widmet sich in einem kürzlich ergangenen Urteil das Bezirksgericht Zürich. [183] Zu beurteilen stand ein Fall, in dem ein Polizeiangehöriger (insgesamt waren es zwei Polizisten und eine Polizistin [184]) eines Tags

ca. um 7 Uhr morgens im Hauptbahnhof Zürich «eine männliche Person mit dunkler Hautfarbe»[185] einer Identitätsprüfung unterzogen hat, da – gemäss seinem Rapport – der Betreffende ihm als verdächtig aufgefallen sei, weil dieser seinen Blick von ihm abgewandt habe, als er ihn als Polizisten erkannt habe und an ihm habe vorbeigehen wollen.[186] Der Kontrollierte unterzog sich der Kontrolle, weigerte sich aber – als Schweizer Bürger – Ausweise vorzulegen.[187] Die Frage der allfälligen Nichtigkeit dieser Personenkontrolle wird ausführlich releviert (Ziff. 5.4 ff.). Nach der Feststellung, dass aufgrund der Judikatur nur in absoluten Ausnahmenfällen von einer nichtigen Personenkontrolle auszugehen sei, wird die Frage gestellt, ob die Feststellung, diese Person habe ihren Blick vom Polizisten abgewandt bzw. einen Bogen um ihn gemacht, die Personenkontrolle zu rechtfertigen vermöge. Leider nicht ganz widerspruchsfrei wird sodann festgehalten, dass es sich nicht «erstellen lässt …, dass die Hautfarbe des Einsprechers ausschlaggebend für die Personenkontrolle war» (a.a.O.). Demgegenüber hat der als Zeuge befragte Polizist jedoch ausgesagt, er habe «eine männliche Person mit dunkler Hautfarbe» einer Kontrolle unterzogen. Dieser wesentliche Punkt erscheint in der rechtlichen Würdigung so nicht mehr. War nun die Hautfarbe ausschlaggebend? Hätte der Polizist die Kontrolle auch durchgeführt, wenn sich eine Person nicht «dunkler Hautfarbe» genau gleich verhalten hätte? Würde diese (zweite) Frage verneint, war die Hautfarbe ausschlaggebend. Damit reduziert sich in diesem Urteil (in der theoretischen Analyse) die Frage nach der Plausibilität eines vernünftigen Anfangsverdachts auf eine Rechtswidrigkeit auf die Differenz: Hat der später Kontrollierte nur (wieder) von den Polizeinagehörigen weggeschaut oder (auch) «einen Bogen» um sie machen wollen? Während nach der zitierten Bundesgerichtspraxis[188] eine Auffälligkeit nach Örtlichkeit (HB Zürich) und Umständen wie das versuchte Ausweichen, um einer Kontrolle zu entgehen, aus Sicht der Polizeiangehörigen, sofern sie von ihrer inneren Haltung her unbelastetet sind, als rechtmässig angesehen werden kann, vermöchte das Abwenden des Blickes allein, nach der hier vertretenen Auffassung, nicht zu genügen; in diesem (zweiten) Fall wäre die Kontrolle als nichtig zu beurteilen. Dass sich der Kontrollierte diskriminiert behandelt fühlte, ist verständlich, was auch im Urteil angetönt wird.[189]

## VI. Verbesserung der Rechtslage für die Praxis de lege ferenda?

[Rz 58] Wie erwähnt,[190] enthält keines der kantonalen Polizeigesetze bisher eine Bestimmung, wonach diskriminierende Behandlungen verboten seien. Wenn gleich dies für die Rechtsverwirklichung aufgrund des verfassungsrechtlichen Diskriminierungsverbotes keine rechtliche Lücke darstellt, könnte eine diesbezügliche Norm im Sinne einer Konkretisierung des Grundsatzes der Verfassungs- und Gesetzmässigkeit allen polizeilichen Verhaltens bzw. als Schranke der Rechtsgrundlagen für polizeiliche Interventionen für die Praxis der Klarheit förderlich sein. Denkbar wäre etwa eine Formulierung:

[Rz 59] «Untersagt ist jede benachteiligende oder bevorzugende Behandlung ausschliesslich aus Gründen insbesondere äusserlich erkennbarer Eigenschaften (z.B. Hautfarbe, Physiognomie), des Geschlechts, des Alters, der Sprache, der sozialen Stellung, der Lebensform, der sexuellen Orientierung, der religiösen, weltanschaulichen oder politischen Überzeugung oder wegen einer körperlichen, geistigen oder psychischen Behinderung».

[Rz 60] An der materiellen Rechtslage änderte sich dadurch nichts. Damit entfiele aber für Identitätsüberprüfungen, die wegen einer negativen inneren Haltung bezüglich «Andersartigkeit» einer Person ausschliesslich auf Grund äusserlich erkennbarer Eigenschaften durchgeführt würden,[191] die gesetzliche Grundlage, womit sie nichtig wären. Ein Mangel Plausibilität für einen vernünftigen Anfangsverdacht führte demgegenüber zur Anfechtbarkeit.

## VII. Die Rechtsanwendung – die Tauglichkeit der Kriterien in der Praxis

[Rz 61] Die Betrachtung zeigt, dass bisher die teilweise in der Rechtswissenschaft, teilweise von Kommissionen wie der Europäischen Agentur für Grundrechte verwendeten Definitionen und Formulierungen, die auch auf diskriminierende

Personenkontrollen Anwendung finden sollen, nicht nur vielfältig, sondern auch widersprüchlich sind. Dabei werden zudem objektive und subjektive Sachverhalte vermischt. Während das Bundesgericht in konstanter Rechtsprechung festhält, dass eine Diskriminierung nur vorliege, wenn allein auf die hier diskutierten Anknüpfungsmerkmale abgestellt werde, [192] wird bspw. im Handbuch der Europäischen Agentur zusammengefasst, «eine Person anzuhalten und zu durchsuchen, die ausschließlich oder überwiegend aufgrund der Rasse, ethnischen Zugehörigkeit oder Religion dieser Person erfolgt», könne als diskriminierendes Ethnic Profiling bezeichnet werden und sei unrechtmäßig. [193] Ausschliesslich oder «überwiegend»? Wie wird «überwiegend» von wem festgestellt? Zudem stelle es eine Diskriminierung dar, «wenn eine Person weniger wohlwollend behandelt wird als eine andere Person, die sich in einer ähnlichen Situation befindet». [194] Wie wird das Mass des Wohlwollens festgestellt und womit verglichen? Ist wohlwollend ein bauchbares Kriterium?

[Rz 62] Solche Formulierungen eignen sich grundsätzlich nicht zur korrekten Lösung einer rechtlich wichtigen Unterscheidung. Sie sind unbestimmt, teilweise gefühlsbetont, v.a. aber widersprüchlich und somit für die Praxis der Rechtsanwendung nicht tauglich, auf die es in erster Linie ankommt.

[Rz 63] Bei der Frage, ob eine Personenkontrolle diskriminierend sei, geht es darum festzustellen, ob hinter dem Fokus auf die der Kontrolle unterworfene Person eine Beeinträchtigung ihrer Menschenwürde, ihre Herabwürdigung, allein auf Grund äusserlich erkennbarer Eigenschaften, d.h. ihrer «Rasse», «ethnischer Herkunft» oder Hautfarbe, steckt. [195] Um dies festzustellen, ist direkt auf die innere Haltung de kontrollieren Polizeiangehörigen abzustellen. Das gilt gleichermassen für das von Bernhard Waldmann als Element einer Diskriminierung postulierte «Pejorative». [196] Es bedarf der Feststellung einer entsprechenden Intention oder Haltung. Das betrifft den subjektiven Sachverhalt.

[Rz 64] Damit wird die Nähe zum strafrechtlichen Rassismustatbestand (Art. 261 bis des Schweizerischen Strafgesetzbuches (StGB) [197]) offenkundig. Der vom Bundesgericht 2014 beurteilte Basler Fall [198] macht deutlich, dass zwischen dem Diskriminierungsverbot nach Art. 8 Abs. 2 BV und dem Tatbestand der Rassendiskriminierung ein Unterschied besteht: Während die übelste Betitelung der kontrollierten Person durch einen Polizeiangehörigen den strafrechtlichen Tatbestand der Rassendiskriminierung nach Auffassung des Bundesgerichts nicht erfüllte (E. 2.5.2, 2.6), stellte sie nach der hier vertretenen Ansicht zweifellos eine Diskriminierung nach Art. 8 Abs. 2 BV im Sinne der Herabwürdigung der Menschwürde einer Person vom Polizisten festgestellt ethnisch algerischer Herkunft dar (E. 2.5.3). [199]

## VIII. Die Bekämpfung diskriminierender Personenkontrollen

[Rz 65] Die Bekämpfung der Diskriminierung bei jeglicher polizeilichen Aufgabenerfüllung, nicht nur bei Personenkontrollen, ist eine ethische und rechtliche Pflicht der zuständigen staatlichen Organe (Art. 35 Abs. 1 und 2 BV). Dabei bildet die Judikatur des Bundesgerichts eine auch in der Praxis taugliche Grundlage. Umzusetzen ist diese Pflicht durch Vorschriften, Selektion, Aus- und Fortbildung sowie die Führung.

### 1. Selektion und Aus- und Fortbildung

[Rz 66] Die Selektion künftiger Polizeiangehöriger legt den Grundstein dafür. Nur Personen mit u.a. einem hohen Mass an Sozialkompetenz, grossem Ausbildungspotential und persönlicher Reife, fern einer fremdenfeindlichen Grundhaltung, eignen sich. [200] Dies bedarf bereits der hinreichend präzisen Rechtsgrundlagen, um ihrerseits keinen Diskriminierungsverdacht aufkommen zu lassen (indirekte Diskriminierung). Die Anforderungen an den Polizeiberuf sind hoch, sehr hoch geworden. Es dient der Qualität des (v.a. künftigen) Polizeipersonals daher nicht, wenn die

Arbeitsbedingungen, namentlich die Besoldung, in Konkurrenz zu ähnlich anforderungsreichen, zumeist aber weit weniger belastenden Berufen verschlechtert werden.

[Rz 67] Die Aus- und permanente Fortbildung auch und gerade in diesem diffizilen Bereich polizeilicher Aufgabenerfüllung[201] liefert die Grundlage dafür, dass die Polizeiarbeit nicht nur auf einem hohen qualitativen Niveau, sondern auch diskriminierungsfrei geleistet wird.[202] Die ECRI[203] hat in ihrem letzten Bericht zwar festgestellt, dass die Ausbildung der Polizeikräfte in der Schweiz nun Ethik und Menschenrechte umfasse, ein neues Lehrmittel hergestellt worden sei und eine zweistündige Klausur zu diesen Themen einschlösse. Trotzdem ist sie damit (sowie mit der entsprechenden Aus- und Weiterbildung der Staatsanwälte und Richter) noch nicht befriedigt.[204] Weitere Anstrengungen sind zu befürworten.

### 2. Führung

[Rz 68] Die konsequente Führung des Polizeipersonals, konzeptionell gut aufgegleist, auf allen Stufen ist unabdingbar für eine möglichst belastbare Gewährleistung der diskriminierungsfreien polizeilichen Aufgabenerfüllung. Das beginnt mit der Gesetzgebung. Ein explizites Diskriminierungsverbot im Polizeigesetz vermöchte mehr Klarheit zu bewirken (vorstehend, VI.). Das wäre schon deshalb vorteilhaft, weil sowohl in der Ausbildung als auch in der Führung das Polizeigesetz «näher» liegt als die BV, die ARK, die Judikatur und Publikationen verschiedener Organe. Zudem sollten abstrakte Begriffe und generelle Situationsbeschreibungen in Dienstvorschriften oder -anweisungen konkretisiert, plausibilisiert werden.

[Rz 69] Zur Führung gehört ein in der Organisationskultur eingebettetes und entwickeltes Sensorium aller, allfällige diskriminierende Verhaltensweisen von Polizeiangehörigen zu bemerken ebenso wie die geeigneten Mittel, sie zuständigenorts bekannt zu machen (Rapportierung, auch whistle blowing). Zudem ist es Teil der Führungsaufgabe, konsequent gegen allfällige Subkulturen («canteen culture») anzugehen, die negativ innere Haltungen beeinflussen oder durch Gruppendruck gar aufoktroyieren können. Fachlich und organisationskulturell wesentlich erscheint der Einbezug von Vertreterinnen und Vertretern von Minoritäten in Aus- und Weiterbildungen. Insgesamt muss dies zusammen bewirken, unverzüglich die notwendigen Korrekturen einzuleiten oder gegebenenfalls auch individuelle Massnahmen zu ergreifen.

[Rz 70] Schliesslich bedarf es eines Systems, durch das diskriminierende Verhaltensweisen mit entsprechenden Sanktionen belegt werden können (Disziplinarwesen[205]). In schwerwiegenden Fällen, die einer nicht leicht beeinflussbaren Haltung entsprechen, muss man sich u.U. auch von ungeeigneten Mitarbeitenden trennen. Wer es nicht begreifen will, hat nicht den richtigen Beruf gewählt.[206] Dies nach Möglichkeit zu vermeiden, ist ebenso schwierige wie unverzichtbare permanente Aufgabe der Führung auf allen Ebenen.

[Rz 71] Zu dieser Führung auf der obersten Ebene gehört indessen auch die Ermöglichung durch die Politik, genügend qualifizierte Kräfte anstellen und behalten zu können.

## IX. Schlussbetrachtung und die Frage der Verantwortungsverteilung

[Rz 72] Die Betrachtung zeigt, dass – mit Ausnahme der bisherigen bundesgerichtlichen Rechtsprechung – die Umschreibungen dessen, was Diskriminierung im Zusammenhang mit Personenkontrollen nach den hier erörterten Anknüpfungskriterien bedeute, weit auseinandergehen und rechtlich nicht zu befriedigen vermögen. Die Grundtypen der Diskriminierungsverbote nach «Rasse» in einem sehr fragwürdigen ethnologischen Sinn verfügen selber über keine scharfen Konturen.[207] Damit wird die Verantwortung von der Politik als Rechtssetzungsorgan und der

Rechtswissenschaft auf die Praktiker verschoben, ohne in genügend klarer Weise vorzugeben, was denn genau gilt. Entscheide, die innert kürzester Zeit und oft unter widrigen Umständen getroffen werden müssen, bedürfen verlässlicher Vorgaben des Rechts. Die durchwegs geforderte Vorhersehbarkeit einer Regelung zur Steuerung des eigenen Verhaltens für alle Rechtsadressaten[208] muss sich für die polizeiliche Arbeit in verlässlichen, begreif- und handhabbaren Rechtsbegriffen spiegeln. Die Verantwortung des Staates, konkretisiert in der Pflicht des Gesetzgebers, unterstützt von der Wissenschaft, ist es, die für die Praxis tauglichen Kriterien zum Schutz der Menschenwürde und der Freiheit ebenso wie zum Schutz der Ordnung des Rechtsstaates als Ganzes verständlich vorzugeben.[209] Das ist hinsichtlich der Rechtssätze für die Vermeidung diskriminierender Personenkontrollen derzeit nicht der Fall. Ein wenig erfreulicher Befund für einen der schwierigsten staatlichen Wirkungsbereiche, in dem Rechtsstaatlichkeit verlässlich und überzeugend gemessen werden können sollte.

---

Dr. iur. Markus H.F. Mohler, ehem. Lehrbeauftragter für öffentliches, speziell Sicherheits- und Polizeirecht an den Universitäten von Basel und St. Gallen, zuvor Kommandant der Kantonspolizei Basel-Stadt, vorher Staatsanwalt; langjähriger Berater (und Unterrichtender) für die DEZA im Bereich von Justiz- und Polizeireform in afrikanischen Ländern und insbesondere in Ländern des Westbalkans (2001–2011).

---

1 Überarbeitete und ergänzte Fassung des an der Tagung des Schweizerischen Kompetenzzentrums für Menschenrechte am 1. Dezember 2016 gehaltenen Einleitungsreferates.

2 Zu dessen Grundlagen: Übersicht: http://www.skmr.ch/de/skmr/index.html; Rahmenvertrag zwischen dem Bund und der Universität Bern: http://www.skmr.ch/cms/upload/pdf/151217_Contrat_cadre_CSDH_2016-2020.pdf; interuniversitäre Vereinbarung: http://www.skmr.ch/cms/upload/pdf/160114_Accord_CSDH_universites_2016-2020.pdf; Struktur: http://www.skmr.ch/de/skmr/struktur/index.html (Alle Websites zuletzt besucht am 17. Februar 2017).

3 Das ist insofern zusätzlich interessant, als auch in der 4. Auflage (Bern 2014) des Allgemeinen Verwaltungsrechts von Pierre Tschannen/Ulrich Zimmerli/Markus Müller, dreier renommierter Autoren dieser Fakultät, dem Polizeirecht eine «Daseinsberechtigung als eigenständige Institute des Verwaltungsrechts» abgesprochen wird. Es gebe «kein spezifisches Wesensmerkmal, das die polizeiliche Verwaltungstätigkeit von irgendeiner anderen Staatstätigkeit abgrenzen liesse. Oder anders: Von der polizeiliche Tätigkeit lässt sich keine rechtliche Aussage machen, die nicht auch für andere Tätigkeiten gelten würde. …» (§ 53, Rz. 24).

4 «Die einzelnen Differenzierungsgründe, die in Art. 14 EMRK aufgeführt sind, erklären sich weitestgehend aus sich selbst heraus», so Christoph Grabenwarter/Katharina Pabel, Europäische Menschenrechtskonvention, 6. Auflage, München 2016, § 26, Rz. 8, was so eben nicht zutrifft.

5 Vgl. Markus H.F. Mohler, Zur Anfechtbarkeit polizeilicher intervenierender Realakte unter dem Gesichtspunkt der Rechtsweggarantie gemäss Art. 29a BV-Justizreform, in: AJP 4/2007, 461 ff.; DERS., Grundzüge des Polizeirechts in der Schweiz, Basel 2012 (nachfolgend: Grundzüge), Rz. 854 ff.

6 Prof. Dr. Marc Bossuyt, Mitglied des UNO-Ausschusses für die Beseitigung von Rassendiskriminierung (CERD), ehem. Präsident des Verfassungsgerichtshofes von Belgien: Le CERD, la Suisse et le profilage racial (http://www.skmr.ch/cms/upload/pdf/161201_Article_Marc_Bossuyt.pdf).

7 Karl Ernst Georges, Lateinisch-deutsches Schulwörterbuch, 10. Auflage, Hannover 1907

8 Bsp. : une personne ne sait pas faire une discrimination entre … et ….. Vgl. auch Bernhard Pulver, L'interdiction de la discrimination, Diss. Neuenburg, Basel 2003, 120 ff.

9 SR 0.101.

10 Später auch durch Art. 1 des 12. Zusatzprotokolls zur EMRK, das von der Schweiz nicht unterzeichnet und auch von zahlreichen andern Staaten nicht ratifiziert worden ist («Artikel 1 – Allgemeines Diskriminierungsverbot [1]Der Genuss eines jeden gesetzlich niedergelegten Rechtes ist ohne Diskriminierung insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der Sprache, der Religion, der politischen oder sonstigen Anschauung, der nationalen oder sozialen Herkunft, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt oder eines sonstigen Status zu gewährleisten. [2]Niemand darf von einer Behörde diskriminiert werden, insbesondere nicht aus einem der in Absatz 1 genannten Gründe.»).

11 Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte, SR 0.103.1.

12 Internationaler Pakt über bürgerliche und politische Rechte, SR 0.103.2.

13 SR 0.104 (im Folgenden: ARK).

14 Yvo Hangarter, Staatliches Handeln im Bereich von Diskriminierungsverboten, in: Stephan Breitenmoser et al. (Hrsg.), Menschenrechte, Demokratie und Rechtsstaat, Liber amicorum Luzius Wildhaber, Zürich/St. Gallen 2007, 1301.

15 «Herkunft, der Rasse, des Geschlechts, des Alters, der Sprache, der sozialen Stellung, der Lebensform, der religiösen, weltanschaulichen oder politischen Überzeugung oder wegen einer körperlichen, geistigen oder psychischen

Behinderung».

16 Georg Müller, Kommentar zur BV 1874, Basel/Zürich/Bern 1996, Art. 8, Rz. 18a. Der zweite Satz von Art. 4 Abs. 1 BV 1874 enthielt ein Privilegierungsverbot, das in Art. 8 Abs. 2 BV 1999 durch ein Diskriminierungsverbot ersetzt wurde, Rainer J. Schweizer, St. Galler Kommentar, 3. Auflage, Zürich/St. Gallen 2014, zu Art. 8, Rz. 46.

17 Botschaft über eine neue Bundesverfassung vom 20. November 1996 (im Folgenden: Botsch. VE 96), BBl 1997 I 1 ff., 142.

18 Bernhard Waldmann, Das Diskriminierungsverbot nach Art. 8 Abs. 2 BV, Habil. Freiburg, Bern 2003, 232 f.

19 Das Völkerrecht kennt selber keinen dem Verfassungsrecht vergleichbaren allgemeinen Gleichstellungssatz: Waldmann (FN 18), 202. Grabenwarter/Pabel (FN 4), § 26, Rz. 25, lassen dies in Bezug auf das 12. ZP zur EMRK (CETS 177, vorstehend FN 10) allerdings offen. Zum allgemeinen Gleichbehandlungsgebot nach Art. 8 BV: Botsch. VE 96 FN (17), 142.

20 BGE 139 I 292 E. 8.2.1 m.w.N., vgl. FN 30.

21 Schweizer (FN 16), Rz. 13; vgl. Waldmann, in Waldmann/Belser/Epiney (Hrsg.), Basler Kommentar zu Art. 8 BV (nachfolgend: BK), Rz. 45 ff. Insofern ist eine Formulierung im Handbuch «Diskriminierendes Profiling» der European Agency for Fundamental Rights (FRA), Luxemburg 2010 (http://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_DE.pdf), unzutreffend: «Diskriminierung im Kontext des Profiling ist üblicherweise eine «direkte» Diskriminierung, die leicht zu erkennen ist, da sie in einer unterschiedlichen Behandlung ohne rechtmäßige Begründung basiert»; sie stimmt auch nicht mit Art. 2 der Richtlinie 2000/43/EG (ABl. L 180 v. 19.7.2000, 22 ff; für die Schweiz nicht massgebend) überein.

22 Hangartner (FN 14), 1302.

23 Waldmann (FN 18), 235.

24 Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, 687 f.

25 Giovanni Biaggini, BV, Art. 8, N 22; Hangartner (FN 14), 1305; Pulver (FN 8), 133 f.; Schweizer (FN 16), Rz. 48.

26 BGE 135 I 49 E. 4.1; Statt vieler: Helene Keller, in: Giovanni Biaggini/Thomas Gächter/Regina Kiener(Hrsg.), Staatsrechte 2. Aufl., Zürich/St. Gallen 2015, § 38, Rz. 45.

27 BGE 139 I 292 E. 8.2.2; BGE 138 I 305 E. 3.3; Schweizer (FN 16), Rz. 48.

28 BGE 135 I 49 E. 4.1.

29 Hangartner (FN 14), 1305; Maya Hertig Randall, Die Situation von Muslimen, insbesondere muslimischen Frauen, in der Schweiz – eine verfassungsrechtliche Einordnung, in: ÖJV, Diskriminierung in der Schweiz und in Österreich (2015), 77; Mohler, Grundzüge (FN 5), Rz. 343 ff.

30 BGE 139 I 292 E. 8.2.1 m.w.N.; BGE 129 I 217 E. 2.1 m.w.N. (Hervorhebung hier). Zur Praxis des BGer Waldmann (FN 18), 246 ff. Vgl. ferner die Umschreibung von Rassendiskriminierung durch die Eidg. Kommission gegen Rassismus EKR (http://www.ekr.admin.ch/themen/d169.html); Albert Scherr, Diskriminierung – wie Unterschiede und Benachteiligungen gesellschaftlich hergestellt werden, 2. Aufl., Wiesbaden 2016, 8, liefert eine andere Definition: «Diskriminierung basiert auf kategorialen, d.h. vermeintlich trennscharfen und eindeutigen Unterscheidungen, mit denen diejenigen markiert werden, die sich in erkennbarer Weise vom angenommenen Normalfall des vollwertigen Gesellschaftsmitglieds unterscheiden. Dieser angenommene Normalfall ist der erwachsene, männliche, physisch und psychisch gesunde Staatsbürger, der zudem kulturell (Sprache, Religion, Herkunft und im Hinblick auf äusserliche Merkmale (Hautfarbe) der Bevölkerungsmehrheit bzw. der dominanten gesellschaftlichen Gruppe angehört. Die für die Diskriminierung bedeutsamen kategorialen Unterscheidungen sind Bestandteil historischer und gegenwärtiger gesellschaftlicher Machtverhältnisse und Ungleichheiten, keine bloss gedanklichen Konstrukte».

31 Im Strafrecht dient dies der Einschränkung der strafrechtlich verpönten Diskriminierung: BGE 140 IV 67 E. 2.5.1.

32 Vgl. Ulrich Häfelin/Walter Haller/Helen Keller/Daniela Thurnherr, Schweizerisches Bundesstaatsrecht, 9. Aufl., Zürich/Basel/Genf 2016, Rz. 744.

33 Jonas Bens, Ethnie als Rechtsbegriff, Kulturanthropologische Problembeschreibungen zum Allgemeinen Gleichbehandlungsgesetz, Aachen 2013, 67, 77 ff.; Matthias Herdegen, Europarecht, 16. Aufl., München 2014, § 6, Rz. 17ff.

34 BGE 140 I 353 E. 7 (Die Diskriminierung eines Pädophilen als psychisch Kranker, der durch eine verdeckte Vorermittlung in einem Chatroom identifiziert worden ist, hat das Bundesgericht abgelehnt. Die verdeckte Vorermittlung sei auf die Verhinderung zahlreicher, sehr unterschiedlicher, schwerer Straftaten ausgerichtet. Es könne somit keine Rede davon sein, die beanstandete Bestimmung stelle eine gegen Art. 8 Abs. 2 BV verstossende Diskriminierung von Personen mit pädophilen Neigungen als psychische Krankheit dar.

35 So kann bspw. die Frage gestellt werden, ob die rein formale Altersbegrenzung (70. Altersjahr) nach Art. 5g und 27 Abs. 1 Bst. b der Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr (VZV, SR 741.51) in dieser Form nicht diskriminierend sei.

36 Vgl. auch Botschaft über den Beitritt der Schweiz zum Internationalen Übereinkommen von 1965 zur Beseitigung jeder Form von Rassendiskriminierung und über die entsprechende Strafrechtsrevision v. 2. März 1992 (BBl 1992 III 269, im Folgenden: Botsch. ARK), 279.

37 Waldmann (FN 18), 248.

38 Waldmann (FN 18), 248 f., 255 ff. Der dazu in der Fn. 215 angefügte Beleg, dass eine Diskriminierung auch ohne benachteiligende Wirkung vorliegend könne, wenn sie von einer entsprechenden Benachteiligungsabsicht getragen gewesen sei, trifft zwar zu, genügt aber nicht für den Umkehrschluss: die pejorative, also herabwürdigende Behandlung als Angriff auf die Wertschätzung einer Person, ist ohne entsprechende individuelle mentale Wahrnehmung bzw. Disposition (wozu auch unbewusste Vorurteilshaltungen zählen) der bezeichnenden Person nicht denkbar. Zu unbewussten Vorurteilshaltungen vgl. Justin Nix/Bradley A. Campbell/Geoffrey P. Alpert, Fatal Shootings by U.S. Police Officers in 2015: A Bird's Eye View, in: The Police Chief (Alexandria/VA), 8/2016, 48 ff.

39 Walter Kälin/Jörg Künzli, Universeller Menschenrechtsschutz, 3. Aufl., Basel 2013, Rz. 1059.

40 Waldmann (FN 18), 250.

41 Vgl. etwa Urteil des EGMR Nachova and others/Bulgaria, no. 43577/98 und 43579/98 vom 6. Juli 2005 § 157.

42 Vgl. Stefanie Schmahl, Gleichheitsgarantien, in: Christoph Grabenwarter (Hrsg.), Enzyklopädie Europarecht (EnzEuR), Bd. 2, Europäischer Grundrechtsschutz, Baden-Baden 2014, 591, spricht von «diskriminierender Haltung des Beamten» unter Verweis auf zahlreiche EGMR-Urteile (Hervorhebung hier). Im Urteil Nachova and others/Bulgaria (FN 41) stellt der EGMR bei der Frage, ob die Tötung von zwei Roma durch einen Militärpolizeioffizier rassistisch motiviert gewesen sei, fest: «the Court does not consider that it has been established that racist attitudes played a role» (§ 158).

43 Hangartner (FN 14), 1307.

44 BGE 142 II 49 E. 6.1 («geschlechtsneutral» in diesem BGE kann ohne Weiteres einem Anknüpfungsmerkmal aus Art. 8 Abs. 2 B gleichgestellt werden); BGE 138 I 217, E. 3.3.3; BGE 136 I 297, E. 7.1; BGE 132 I 49, E. 8.1 m.w.H.; Schweizer (FN 16), Rz. 51. Vgl. auch Art. 2 Abs. 1 und 2 der Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 (FN 21), Art. 2 Abs. 2 Bst, b mit einer etwas anderen Formulierung als hier.

45 ZH, Art. 11 Abs. 2; BE, Art. 10 Abs. 1; FR, Art. 8 Abs. 1 (ohne Anknüpfungskriterien); BS, § 8 Abs. 2; SH, Art. 11 Abs. 1; AR, Art. 5 Abs. 2; SG, Art. 2 Bst. a («Schutz vor Diskriminierung», ohne Anknüpfungskriterien); VD, art. 10 al. 2; NE, art. 8 al. 1; GE, art. 15 al. 2 (alle 3 zit. welschen Kantone: «ne doit subir de discrimination», alle Kantonsverfassungen in SR 131.2xx)

46 UR, Art. 11 Abs. 2; NW, Art. 2 Abs. 2; GL, Art. 4 Abs. 2; BL, § 7 Abs. 2; AG, Art. 10 Abs. 2; TI, Art. 7 Abs. 1; JU Art. 6 Abs. 2 («ni subir préjudice ni tirer avantage»).

47 AI; Art. 2 Abs. 1 («Gleichheit der Bürger und der Gleichberechtigten»); TG Art. 3.

48 GR, Art. 2.

49 SG 510.100.

50 Hervorhebung hier. Vgl. dazu die inhaltlich gleichlautende Ziff. 40 der Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics (https://wcd.coe.int/ViewDoc.jsp?p=ℜf=Rec(2001)10⟪uage=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColor

51 RS 551.1.

52 Kälin/Künzli (FN 39), Rz. 59; BK (FN 21), Art. 8, Rz. 67.

53 BK (FN 21), Art. 8, Rz. 69.

54 René Rhinow/Markus Schefer/Peter Übersax, Schweizerisches Verfassungsrecht, 3. Auflage, Basel 2016, Rz. 1914.

55 Pulver (FN 8), 213; vgl. auch Bens (FN 33), 41 mit Hinweis auf Franz Boas.

56 BK (FN 21), Art. 8, Rz. 69.

57 Zur Herkunft der Rassentheorie s. Patrick Thornberry, The International Convention on the Elimination of All Forms of Racial Discrimination, Oxford Commentary on International Law, Oxford 2016, 5 ff. Vgl. Schmahl (FN 42), 590. Siehe aber auch das Statement on the Nature of Race and Race Differences, UNESCO, Paris 1951 (http://unesdoc.unesco.org/images/0012/001229/122962eo.pdf) in dem die Existenz menschlicher Rassen nicht a priori negiert wird; sodann die Erklärung der Generalkonferenz der UNESCO über "Rassen" und rassistische Vorurteile vom 27. Oktober 1978 (https://www.unesco.de/infothek/dokumente/unesco-erklaerungen/erklaerung-rassist-vorurteile.html), an deren Übersetzung ins Deutsche redaktionelle Änderungen vorgenommen wurden, um die Begriffe «Rassenvorurteile» und «Rassendiskriminierung zu vermeiden.

58 Thornberry (FN 57), 22; vgl. auch Kathrin Monen, Das Verbot der Diskriminierung, Diss. Düsseldorf 2006/7, Baden-Baden 2007, 91. Nach Bens (FN 33) ist der Begriff der «Rasse» ein biologistisch konnotiertes, kognitiv-ideologisches Konstrukt, 69 f.

59 Richtlinie 2000/43/EG des Rates (FN 44), Erw. 6. Die American Athropological Association (AAA) distanzierte sich 1998 in einer Erklärung vom Begriff «Rasse»: «No human is born with a built-in culture or language. Our temperaments, dispositions and personalities, regardless of genetic propensities, are developed within sets of meanings and values that we call culture». 1999 AAA Statement on race, American Anthropologist, 100(3) 712 f. (zit. nach Bens [FN 33], 41.

60 BK (FN 21), Art. 8, Rz. 70; vgl. auch Jörg Paul Müller, Grundrechet in der Schweiz, 3. Aufl., Bern 1999, 420; Müller/Schefer (FN 24), 718.

61 Schmahl (FN 42), 590.

62 Kälin/Künzli (FN 39), Rz. 1059. Hier fällt auf, dass die Umschreibung von «Rasse» nicht nur auf unterschiedliche physische oder kulturelle Eigenschaften Bezug nimmt, sondern auch gleich («und») auf das Empfinden von Minderwertigkeit, was m.E. nicht richtig sein kann, da damit der (deutschsprachige) Diskriminierungsansatz miteinbezogen wird.

63 Ebenso Marcel Alexander Niggli, Rassendiskriminierung: ein Kommentar zu Art. 261 bis StGB und Art. 171c MStG, 2. Aufl., Zürich 2007, Rz. 619 (Rasse sei ein biologischer Begriff).

64 Die nationale Herkunft dürfte jedoch kaum den biologischen Eigenschaften zugerechnet werden können.

65 Monen (FN 58), 91. «Lebewesen» trifft hier gerade nicht zu, da damit auch andere als Menschen erfasst werden, die sich als Rassen sehr wohl unterscheiden.

66 BK (FN 21), Art. 8, Rz. 69

67 Niggli (FN 63), Rz. 621 ff.

68 Bens (FN 33), 40 f. Vgl. Dazu aber nachfolgend Rz. 36 der Vermerk betr. den Einbezug genetischer Merkmale in der KV BS.

69 BGE 138 II 641 E. 4.3.

70 Vgl. auch Luc de Heusch, L'ethnie. The vicissitues of a concept, in: Social Anthropology (2000), 8, 99, und Bens (FN 33), 69, und Durban Declaration (A/CONF.189/12, http://www.un-documents.net/durban-d.htm), Ziff. 7 u.a.

71 NZZ am Sonntag, 14. November 2016, 23.

72 Das wäre nach schweizerischem Recht unter «soziale Stellung» in Art. 8 Abs. 2 BV zu subsumieren und somit eine Diskriminierung.

73 Vgl. zur Unbestimmtheit: BGE 140 IV 67 E, 2.2.4 und 2.3. Müller/Schefer (FN 24), 720 f. («In diesem Sinn erscheint das Verbot der Rassendiskriminierung in der BV als Grundtyp der Diskriminierungsverbote, ohne selber schon über scharfe Konturen zu verfügen.»).

74 Vgl. aber BGE 140 IV 76, E. 2.4 («wegen» ist auch dort in Anführungszeichen gesetzt). «Wegen» bestätigt im Grund genommen das Bestehen von verschiedenen Rassen unter den Menschen, was ja gerade abgelehnt wird. «Aus Gründen» verweist demgegenüber sprachlogisch auf eine solche Behauptung.

75 Bens (FN 33), 68.

76 Gegenteiliger Ansicht Scherr (FN 30).

77 Vgl. statt mehrerer: Schmahl (FN 42), 590.

78 Thornberry (FN 57), 22.

79 So u.a. auch Schmahl (FN 42), 590. Der EGMR verwendet stereotyp «la race ou l'origine ethnique»: vgl. Urteil des EGMR Biao/Denmark no 38590/10 vom 24. Mai 2016, §§ 66, 68, 96, 102.

80 Etymologisch von altgr. ethnos (Volk, Volksstamm) stammend; zum ersten Mal 1895 als Synonym oder «Ablösung» von «Rasse» verwendet; zur Geschichte des Begriffs «Ethnie» und der andauernden Auseinandersetzungen um das konstituierende Konzept: de Heusch (FN 70), 99 ff.; Bens (FN 33), 1, 24. Dieser sei auch ein Kampfbegriff sozialer Bewegungen der 2. Hälfte des 20. Jahrhunderts, 4.

81 Ethnische Zugehörigkeit werde auch durch genetische Abstammung vermittelt, was eine klare Trennung von Rasse und Ethnie verunmögliche (Bens [33], 73 m.w.N.) – andererseits aber die Existenz unterschiedlicher Rassen gerade abgelehnt wird (vorstehend 1.), vgl. dazu Bens (FN 33), 69 f., 94.

82 Bens (FN 33), 25 ff.

83 Auch «ganz Integrierte» können sich, unabhängig von der Fremdwahrnehmung Dritter, immer noch als Zugehörige einer abstammungs- oder kulturbedingten Gruppe zählen oder eben auch nicht mehr. Vgl. dazu auch Bens (FN 33), 75.

84 Vgl. Bens (FN 33), 75.

85 Vgl. BGE 133 IV 308 E. 9.3.3 («Stiefel von der Art, wie sie nach landläufiger Auffassung auch von «Neonazis» beziehungsweise «Rechtsextremen» getragen werden.»). Das bezieht sich auf eine Parallelwertung in der Laiensphäre (BGE 129 IV 238 E. 3.2.2), die als Tatbestandsmerkmal, zumal im Strafrecht, doch sehr heikel sein könnte. Zwar müssen auch landläufige Kategorien von der Rechtswissenschaft berücksichtigt werden, damit sich diese nicht von den Rechtsadressaten (zu) weit entfernt, doch können sie allein nicht genügen, sondern müssen auf ihre Tauglichkeit als hinreichend bestimmte Begriffe in generell-abstrakten Normen geprüft werden. Vgl. dazu auch Urteil des Bundesgerichts 6B_8/2014 vom 22. April 2014 mit seinen philologischen Betrachtungen zur Bedeutung eines Ausdrucks in der Parallelwertung der Laiensphäre.

86 Bens (FN 33), 75.

87 Vgl. Bens (FN 33), 13.

88 Ernst Kramer, Juristische Methodenlehre, 5. Aufl. Bern/Wien/München 2016, 59 f.

89 Bens (FN 33), 19, 21, 27.

90 Vgl. FN 19.

91 Die Schauspielerin, Schriftstellerin und Herausgeberin einer Zeitschrift Meghan Markle, eine Frau, deren Eltern unterschiedlicher Hautfarbe sind, beklagte sich in einem Artikel « I'm More Than An 'Other'» darüber, dass sie immer wieder gefragt werden, WAS sie sei, also gemeint: weiss oder schwarz (http://www.elleuk.com/life-and-culture/news/a26855/more-than-an-other/).

92 Vgl. Waldmann (FN 18), 244 (unsinniger Prüfungsschritt: «ab wann ein Mensch als 'weiss' gilt und daher nicht mehr als diskriminiert im Sinne des Gesetzes betrachtet werden kann, obwohl die in Frage stehende Behandlung ganz offensichtlich mit der Hautfarbe des Betroffenen zusammenhängt.»).

93 Näheres zu «Putativ-Diskriminierung» bei Bens (FN 33), 98.

94 Botsch. VE 96 (FN 17), 143.

95 A.a.O. Verwiesen wird nur darauf, dass sich die Unzulässigkeit der Diskriminierung nach «Rasse» aus keinem andern Grundrecht ergebe. Auch im EU-Recht «gibt es keine allgemein verbindliche Definition von ‹Rasse›»: Schmahl (FN 42), 589 m.w.N.

96 FN 13.

97 Botsch. ARK (FN 36), 279.

98 FN 17, 142.

99 Vgl. dazu vorstehend Rz. 28 [II., 2.]

100 Vgl. FN 97.

101 Botsch. ARK (FN 36), 311.

102 TG und VS.

103 LU, Art. 10 Abs. 2.

104 SZ, § 10; GR, Art. 7.

105 FR, Art. 9 Abs. 1; SH, Art. 11 Abs. 1; SG, Art. 2 Bst. b.

106 Denise Buser/Michael Albrecht (Hrsg.), Die Entstehung der Baselstädtischen Verfassung vom 23. März 2005, Basel 2010, 11 f.

107 Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin, SR 0.810.2 (Art. 11 «Jede Form von Diskriminierung einer Person wegen ihres genetischen Erbes ist verboten.»).

108 Markus Schefer/Alexander Ziegler, Verbote der Diskriminierung (§ 8 Abs. 2 KV), in: Denise Buser (Hrsg.), Neues Handbuch des Staats- und Verwaltungsrechts des Kantons Basel-Stadt, Basel 2008, 93 ff.

109 Trotz der sich widersprechenden Theorien müsste jemand in dessen Bewusstsein darauf abstellen, dass bspw. die Hautfarbe (z.B. «nicht weiss») genetisch bedingt sei und deswegen jemanden herabwürdigend behandeln.

110 Kein Verweis auf die übergeordnete Rechtsordnung, die BV oder KV findet sich nur in den PolG NW (911.1), SG (sGS 451.1) und SZ (SRSZ 520.110), sondern lediglich einer auf die Massgeblichkeit des Verhältnismässigkeitsprinzips (was immerhin einen Bezug in persönlicher Hinsicht als Schranke eines Eingriffs in [Grund-] Rechte nach zwei der drei Prüfkriterien hinsichtlich der persönlichen Schutzbereichs erlaubt: «erforderlich» und «geeignet»).

111 GL (GS VA 11/1), Art. 6; GR (RB 6130.000), Art. 5; JU (RS 551.1), Art. 34; NE (RSN 561.1), Art. 1 Abs. 1 (KV), Abs. 2 (Grundrechte); OW (GDB 510.1), Art. 8 Abs. 1 (Rechtsordnung), Abs. 2 (Grundrechte und Menschenwürde); SH (Syst.Nr. 354.1), Art. 18 Abs. 1 (verfassungsmässige Rechte); TG (RB 551.1), Art. 12 Abs. 1 (Rechtsordnung), Abs. 2 (verfassungsmässige Rechte und Menschenwürde); VD (RS 133.11), Art. 13 ( im Gelöbnis: «fidèle à la Constitution fédérale et à la Constitution du canton de Vaud); VS (RS 550.1), Art. 11 (im Gelöbnis: «der Verfassung treu zu bleiben»); ZG (BGS 512.1), § 9 («im Rahmen der Gesetzgebung des Kantons und des Bundes); ZH (LS 550.1), § 8 Abs. 1 (Rechtsordnung), Abs. 2 (verfassungsmässige Rechte und Menschenwürde).

112 AG (SAR 531.200), Art. 25 Abs. 1; AR (bGS 521.1), Art. 5; BL (SGS 700), § 15; BS (GS 510.100), § 7und § 22 (Gelöbnis der Pflichterfüllung «ohne Ansehen der Person und vorurteilslos»); FR (BDLF 551.1), Art. 30a; GE (F 105), Art. 45 Abs. 1; GL (GS VA 11/1), Art. 6; GR (RB 613.000), Art. 6; LU (SRL 350), Art. 5; NE (RSN 561.1), Art. 40 Abs.1; SH (Syst. Nr. 354.100), Art. 18 Abs. 1; SO (BGS 511.11), § 25; UR (RB 3.8111), Art. 6.

113 Neben den spezifischen Abkommen zum Schutz der Grundrechte (vgl. FN 11, 12, 13), dem Übereinkommen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe (SR 0.105), dem Übereinkommen über die Rechte des Kindes (SR 0.107), dem Übereinkommen zur Beseitigung jeder Form von Diskriminierung der Frau (SR 0.108), dem Abkommen über die Rechtsstellung der Flüchtlinge («Genfer Flüchtlingsabkommen», SR 0.142.30) samt den Zusatzprotokollen I (SR 0.518.521) und II (SR 0.518.522) gehören auch zahlreiche Abkommen zur Bekämpfung spezifischer Kriminalitätsformen dazu, deren Umsetzung in die Praxis aus der Perspektive des grundrechtlichen Diskriminierungsverbotes schwierige Situationen entstehen lassen können, z.B. (ohne Vollständigkeit): Übereinkommen zur Bekämpfung des Terrorismus (SR 0.353.21, 0.353.22, 0.353.23), Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität («Palermo-Abkommen» oder «UNTOC»; SR 0.311.54), Zusatzprotokoll dazu gegen die Schleusung von Migranten auf dem Land-, See- und Luftweg (SR 0.311.541), Zusatzprotokoll dazu zur Verhütung, Bekämpfung und Bestrafung des Menschenhandels, insbesondere des Frauen- und Kinderhandels (SR 0.311.542).

114 Vgl. SR 0.360.xxx.

115 Z.B. Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (SR 0.311.40), Übereinkommen zur Bekämpfung des Menschenhandels (SR 0.311.543), Europäisches Übereinkommen über Gewalttätigkeiten und Ausschreitungen von Zuschauern bei Sportanlässen, insbesondere bei Fussballspielen (SR 0.415.3).

116 SR 0.362.31 mit sehr vielen Weiterentwicklungen des Schengen-Besitzstandes (vgl. https://www.bj.admin.ch/dam/data/bj/sicherheit/schengen-dublin/uebersichten/weiterentwicklungen-schengen-d.pdf. oder http://www.recht-sicherheit.ch/international-Schengen/articles/schengen-besitzstand-weiterentwicklung.html);.

117 SR 0.142.392.68 mit Weiterentwicklungen des Dublin/Eurodac-Besitzstandes (https://www.bj.admin.ch/dam/data/bj/sicherheit/schengen-dublin/uebersichten/weiterentwicklungen-dublin-d.pdf).

118 Mohler, Grundzüge (FN 5), Rz. 47 ff., 154 ff., 166 ff.

119 Mohler, Grundzüge (FN 5), Rz. 24 ff.; Ders., Ethik in der Polizei, in; János Féherváry/Wolfgang Stangl (Hrsg.), Menschenrecht und Staatsgewalt, Wien 2000 (nachfolgend: Ethik), 201 ff.

120 Bezüglich Personenkontrollen z.B.: BGE 109 Ia 146 E. 4b («L'interpellation de police doit répondre à des raisons objectives minimales, telles l'existence d'une situation troublée, la présence de l'intéressé dans le voisinage de lieux où vient de se commettre une infraction, sa ressemblance avec une personne recherchée, son insertion dans un groupe d'individus dont il y a lieu de penser, à partir d'indices si faibles soient-ils, que l'un ou l'autre se trouverait dans une situation illégale impliquant une intervention policière»).

121 BGE 136 I 87 E. 5.1 ; 109 Ia 146, E. 4.b («…la simple interpellation de police à fin de vérification d'identité… ne constitue pas en soi une atteinte très sensible à la liberté personnelle».

122 BGE 124 I 85 E. 2b.

123 Hinsichtlich der Problematik der Formulierung dieser polizeilichen Zielsetzung hat das Bundesgericht (im Zusammenhang mit Videoüberwachungen) festgestellt, es handle sich um ein «Schlagwort» (BGE 136 I 87 E 8.3).

124 Vgl. bspw. Art. 27 Abs. 1 PolG BE; § 34 Abs. 1 PolG BS; Art. 47 al. 1 loi sur la pol GE; § 21 Abs. 1 PolG ZH. BGE 142 I 121 E. 3.2.

125 Vgl. Art. 27 Abs. 2 PolG BE; § 34 Abs. 2 PolG BS; art. 47 al. 1 et 2 loi sur la pol GE; § 21 Abs. 2 PolG ZH.

126 Vgl. BGE 137 I 176, E.7.3.3; Mohler, Grundzüge (FN 5), Rz. 386 ff.

127 BGE 136 I 87 E. 5.2.

128 BGE 136 I 87 E. 5.2.

129 Mohler, Grundzüge (FN 5), Rz. 386.

130 Mohler, Grundzüge (FN 5), Rz. 123.

131 Vom 16. Dezember 2006, SR 142.20, Art. 9 Abs. 1 («Die Kantone üben auf ihrem Hoheitsgebiet die Personenkontrolle aus.») i.V.m. Art. 46 Abs. 1 BV.

132 SR 122.

133 Vom 27. Juli 2009, No. 1493/2006, Williams Lecraft v. Spain (A/64/40, vol. II (2009) Annex VII ff., page 295 ff. (http://www.bayefsky.com/pdf/spain_t5_iccpr_1493_2006.pdf.), Ziff. 7.2. Näheres dazu nachstehend Rz. 50 (Bst. a) [IV., 2. a.]

134 Art. 5 Abs. 2 BV.

135 Benjamin Schindler, Verwaltungsermessen, Habil. Zürich/St. Gallen 2010, N. 418 ff., 435; Mohler (FN 5), Rz. 124, 335 je m.w.H.

136 BGE 136 I 87 E. 5.2.

137 Vgl. Rebekah Delsol, Good Practices, Learning from the UK Experience, Referat gehalten an der SKMR Tagung vom 1. Dezember 2016 (http://www.skmr.ch/cms/upload/pdf/161201_Presentation_Rebekah_Delsol.pdf) mit Verweis auf Code A (2014/15) des UK Home Office.

138 BGE 132 I 49 E. 8.1.

139 Vorstehend I., 2.

140 BGE 132 I 49 E. 8.1.

141 BGE 127 I 6 E. 5b (unter Verweis auf J.P. Müller).

142 Müller/Schefer (FN 24), 4.

143 Auch wenn dieser (weshalb?) aus dem Englischen übernommene Ausdruck in seiner Offenheit bzw. Ungenauigkeit selber problematisch ist. Er stimmt auch keineswegs darin überein, was nach der schweizerischen Rechtsordnung mit Persönlichkeitsprofil gemeint ist.

144 Vgl. den in diesem Zusammenhang als good practice bezeichneten (FN 137) Code A Exercise by Police Officers» statutory Powers of Stop and Search (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414195/2015_Code_A_web-19-03-15.pdf): no. 2.2. «Reasonable grounds for suspicion is the legal test which a police officer must satisfy before they can stop and detain individuals…).

145 (FN 144).

146 «linked to accurate and current intelligence or information, relating to articles for which there is a power to stop and search…»

147 «reliable information or intelligence that members of a group or gang habitually carry knives unlawfully or weapons or controlled drugs, and wear a distinctive item of clothing or other means of identification in order to identify themselves…»

148 «reasonable suspicion may also exist without specific information or intelligence on the basis of the behaviour of a person. … For example … trying to hide something. … An officer who forms the opinion that a person is acting suspiciously or that they appear to be nervous must be able to explain, with reference to specific aspects of the person's behaviour or conduct which they have observed why they formed that opinion. … A hunch or instinct which cannot be explained or justified to an objective observer can never amount to reasonable grounds».

149 Vorstehend I., 2.

150 Vgl. nachstehend IV., 2. a, (Rz. 50).

151 Art. 115 Abs. 1 Bst. a, b. und d i.V.m. Art. 7 AuG.

152 BGE 131 IV 174 E. 4.1.

153 http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx.

154 UN Menschenrechtsausschuss (FN 174), § 7.2.

155 Vgl. Art. 22 i.V. mit Art. 23 Bst. a i) der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (ABl. L 77 v. 23. März 2016 1 ff.; von der Schweiz übernommen: SR 0.362.380.067 [AS 2016 1947]); BGE 138 IV 69 E. 3.4.2.1 (noch zum vormaligen Schengener Grenzkodex, der diesbezüglich gleich lautete).

156 BGE 136 I 87 E. 5.2.

157 Müller/Schefer (FN 24), 721.

158 Vgl. Art. 11 Bst. g, i und m der Verordnung über das automatisierte Polizeifahndungssystem (RIPOL-Verordnung, SR 361.0) und Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung, SR 362.0), Anhang 3, Ziff. 2.2.1, und Anhang 4, Ziff. 2.

159 Vgl. Agentur der Europäischen Union für Grundrechte, EU-MIDIS, Erhebung der Europäischen Union zu Minderheiten und Diskriminierung, Luxemburg 2011.

160 FN 21, 30.

161 Vgl. Bossuyt (FN 6), 4.

162 Staatsanwaltschaft Basel-Stadt, Polizeiliche Kriminalstatistik (PKS), Jahresbericht Basel-Stadt 2015, Statistiken 2.9.4.1. und 2.9.4.2.

163 BFS/KKJPD, Polizeiliche Kriminalstatistik (PKS), Jahresbericht 2015, Neuenburg 2016, Statistik 3.8.4.2.

164 Nach dem Handbuch «Diskriminierendes Profiling (FN 21), 35: «Die «Trefferquote» bezeichnet den Anteil der Personenkontrollen und Durchsuchungen, bei denen Beweise für rechtswidriges Verhalten gefunden werden…».

165 PKS 2015 (FN 163), Statistik 2.4.2.

166 BGE 139 I 292 E. 8.2.1; 139 I 169 E. 7.2.1; 138 I 217 E. 3.3.3; 136 I 297 E. 7.1.

167 BGE 136 I 87 E. 5.2 («Umstände»).

168 (FN 21) Ziff. 2.5, S. 25 («Verglichen mit anderen Gruppen hat diese Vorgehensweise in der Praxis jedoch vor allem eine eher negative Auswirkung auf eine bestimmte ethnische, religiöse oder Rassengruppe (z. B. 60% der Bevölkerung, die in der Stadt X zu dieser Zeit mit dem Auto unterwegs sind, haben eine afrokaribische Abstammung, während dieser Wert in der Umgebung nicht mehr als 30% beträgt.»). Man beachte auch die in diesem Zusammenhang doch befremdliche Verwendung des Ausdrucks «Rassengruppe».

169 Vgl. BGE 140 I 53 E. 7.

170 EU Observer, 23. Februar 2015 (https://euobserver.com/justice/127737).

171 Vgl. Vorstehend Rz. 21.

172 Vgl. ECRI General Policy Recommendation N° 11 on combating racism and racial discrimination in policing (adopted on 29 June 2007, at ECRI's 43rd plenary meeting), Paragraph 1: «'The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin in control, surveillance or investigation activities'». (Hervorhebung d. Autor.)

173 BGE 135 I 49, E. 6.

174 BGE 136 I 87 E. 5.2 («aus bloss vorgeschobenen Gründen»).

175 Vgl. dazu die inhaltlich gleichlautende Formulierung in der Entscheidung des UN Menschenrechtausschusses A/64/40, vol. II (2009) Annex VII.FF., page 295 ff. Communication No. 1493/2006, Williams Lecraft v. Spain (Views adopted on 27 July 2009, Ninety-sixth session), § 7.4 («In the circumstances, the Committee can only conclude that the author (= Beschwerdeführerin) was singled out for the identity check in question solely on the ground of her racial characteristics and that these characteristics were the decisive factor in her being suspected of unlawful conduct.» Hervorhebung d. Autor); ferner: Mohler, Ethik (FN 119), 212.

176 Urteil des Bundesgerichts 6B_727/2016 vom 21. Oktober 2016, E. 3.

177 Jürg Martin/Jan Seltmann/Silvan Loher, Die Verfügung in der Praxis, 2. Auflage, Zürich/Basel/Genf 2016, 248.

178 Urteil des Bundesgerichts 5A_950/2014 vom 16. April 2015 E. 3.7.4.

179 BGE 136 I 87 E. 5.2.

180 BGE 109 Ia 146 E. 4b.

181 Stefan Heimgartner, in: Marcel A. Niggli/Hans Wiprächtiger, Basler Kommentar Strafrecht, Bd. II, 3. Auflage, Basel 2013, vor Art. 285 ff. Rz. 19.

182 Urteil des Bundesgerichts 6B_727/2016 vom 21. Oktober 2016, E 3; vgl. Heimgartner (FN 180), Rz. 19.

183 Geschäfts-Nr. GC160218-L/U, Urteil v. 7. November 2016. Zum Zeitpunkt der Drucklegung dieses Beitrages ist das Urteil noch nicht rechtskräftig; Das Urteil wurde ans Obergericht weitergezogen.

184 Urteil (FN 182), Ziff. 4.2.1.

185 Urteil (FN 182), Ziff. 4.3.1.

186 Urteil (FN 182), Ziff. 4.3.3.

187 Seine Effekten wurden wegen der Weigerung schliesslich auf Ausweisschiften durchsucht, der Kontrollierte sodann angezeigt, mit Strafbefehl vom Stadtrichteramt mit CHF 100 gebüsst, was vom Bezirksgericht bestätigt worden ist.

188 Vorstehend, IV., 2. a (BGE 136 I 87 E. 5.2.).

189 Nachfolgend stellt sich die Rechtsfrage, ob sich der Kontrollierte als seit Jahren legal in der Schweiz lebend und offenbar durch viele gleichgelagerte Kontrollen erfahren nicht i.S.v. Art. 14 StGB rechtmässig verhielt, da er die offenkundige Unrechtmässigkeit der Kontrolle aus seiner Sicht annehmen durfte. Vgl. Heimgartner (FN 180), Rz. 26, der in solchen Fällen einen Sachverhaltsirrtum annimmt.

190 Vorstehend, Ziff. I., 4.

191 Vgl. vorstehend, Ziff. IV, 4.

192 Vorstehend I., 1., IV., 1. und FN 166.

193 FN 21, S. 69.

194 A.a.O.

195 BGE 132 I 49, E. 8.1.

196 FN 37.

197 SR 311.0.

198 Urteil des Bundesgerichts 6B_715/2012 vom 6. Februar 2014.

199 Nur ein «pied noir» nach der französischen Definition wäre nicht auch ethnisch algerischer Herkunft. Vgl. die Verurteilung von Wilders in den Niederlanden wegen Rassendiskriminierung und Beleidigung der Marokkaner als Bevölkerungsgruppe (NZZ v. 12. Dezember 2016, 3).

200 Mohler, Ethik (FN 119), 208.

201 Mohler, Grundzüge (FN 5), V (Leitsatz).

202 European Commission against Racism and Intolerance (ECRI), General Policy Recommendation N° 11 on combating racism and racial discrimination in policing (adopted on 29 June 2007, at ECRI's 43rd plenary meeting), Recommendation 4: «To train the police on the issue of racial profiling and on the use of the reasonable suspicion standard.» Rassistische Diskriminierung in der Schweiz, Bericht der Fachstelle für Rassismusbekämpfung 2014 (http://www.ekr.admin.ch/pdf/Rassistische_Diskriminierung_in_der_Schweiz.pdf), Ziff. 6.2.8.

203 Vgl. FN 201.

204 ECRI-Bericht über die Schweiz (fünfte Prüfungsrunde), verabschiedet am 19. Juni 2014, veröffentlicht am 16. September 2014 (https://www.edi.admin.ch/edi/de/home/fachstellen/frb/internationales/ecri.html), Ziff. 66. Im Zusammenhang mit dem weiten Ermessensspielraum, welchen die Polizei bei Personenkontrollen geniesse, stellt sie fest: «Eine Person kann ohne konkreten Verdacht angehalten werden», was der Polizei einen enormen Ermessensspielraum gebe; dabei interpretiert sie das von ihr zitierte Bundesgerichtsurteil 6B_53/2013 vom 8. Juli 2013 E. 2.2, falsch (vgl. dazu Mohler, Grundzüge [FN 5], Rz. 386, und BGE 137 I 176 E. 7.3.3, BGE 109 Ia 146 E 4b).

205 Vgl. Schlussbemerkungen des Comité pour l'élimination de la discrimination raciale (CERD) 2008 (https://www.eda.admin.ch/content/dam/eda/fr/documents/aussenpolitik/internationale-organisationen/Cerd_Schlussempfehlungen_UNO-Ausschuss_fr.pdf), Ziff. 16

206 Vgl. Beispiel in: Beratungsnetz für Rassismusopfer, Rassismusvorfälle aus der Beratungspraxis Januar bis Dezember 2015, Bern Juni 2016 (http://www.ekr.admin.ch/pdf/rassismusbericht_2015_web_d.pdf), 10. Mohler, Ethik (FN 119), 212.

207 Müller/Schefer (FN 24), 718, 720.

208 Mohler, Grundzüge (FN 5), Rz. 153 m.H.

209 Peter Saladin, Verantwortung als Staatsprinzip, Bern 1984, 210 ff.

Bundesamt für Justiz
Bundesrain 20
3003 Bern

**David Rosenthal**
lic. iur., Counsel

**Homburger AG**
**Prime Tower**
**Hardstrasse 201 | CH–8005 Zürich**
**Postfach 314 | CH–8037 Zürich**

T +41 43 222 10 00
F +41 43 222 15 00
david.rosenthal@homburger.ch

4. April 2017

## Vernehmlassungseingabe Revision DSG

Sehr geehrte Damen und Herren

Mit dieser Vernehmlassungseingabe nimmt der Unterzeichnete Stellung zum Vorentwurf für ein revidiertes Datenschutzgesetz (**DSG**) vom 21. Dezember 2016. Sie erfolgt persönlich.

Der Unterzeichnete anerkennt, dass die revidierte Konvention 108 des Europarats (die **Konvention**) eine Revision des DSG im Bereich der privaten Datenbearbeitung zwar erforderlich ist, er ist jedoch der Ansicht, dass die Vorlage noch wesentlich Überarbeitung bedarf. Manche der Bestimmungen werden sich in der Praxis so, wie sie im Vorentwurf formuliert sind, nicht sinnvoll umsetzen lassen oder eine unnötige Bürde für die betroffenen Datenbearbeiter darstellen, weil sie dem Datenschutz nicht wirklich zuträglich oder unverhältnismässig ist. Der Unterzeichnete verweist im Einzelnen auf die in seinem Aufsatz vom 20. Februar 2017 in der Fachpublikation *Jusletter* gemachten Ausführungen (Beilage), die hiermit zum integralen Bestandteil dieser Eingabe erklärt wird.

Die wichtigsten Kritikpunkte sind zusammengefasst:

1. Der Begriff des Profiling (**Art. 3**) sollte gestrichen werden, mindestens jedoch das manuelle Profiling. Er bringt keinen Mehrwert, da das DSG ohnehin einen risikobasierten Ansatz verfolgt. An heikle Datenbearbeitungen sind auch ohne diesen Begriff höhere Anforderungen zu stellen als an wenig heikle. Die Konvention verlangt eine Regelung wie im DSG nicht.

2. Biometrische Daten dürfen nur dann besonders schützenswert sein, wenn sie dem Zweck der Identifikation dienen, und nicht schon, wenn die Identifikation möglich ist (**Art. 3**). Sonst werden beispielsweise unzählige völlig normale Foto, Video oder Tonaufnahmen zu solchen Daten.

3. Es ist in der Botschaft korrekt zu erläutern, wann eine Einwilligung ausdrücklich ist (**Art. 4**). Hierzu wird auf die Ausführungen in der Beilage verwiesen. Die Erläuterungen zum Vorentwurf sind falsch.

4. Die Meldepflichten bei der Bekanntgabe ins Ausland in "Ausnahmefällen" ist praxisfern und bringt keinen Mehrwert (**Art. 6**). Bei der Rechtfertigung des Vertrags sind Drittinvolvierte am Vertrag zu erfassen und bei der Rechtfertigung der Durchsetzung von Rechtsansprüchen die Einschränkung auf Gerichte und Verwaltungsbehörden zu streichen (analog DSGVO).

5. Es gibt keinen Grund, dem Bundesrat das Recht einzuräumen, Auftragsdatenbearbeitern weitere Pflichten aufzuerlegen (**Art. 7**). Ihnen kommen zudem zuviele der Pflichten im neuen DSG zu, für die sie kraft ihrer Subordinationsstellung gar nicht vernünftig verantwortlich sein können (z.B. **Art. 16**).

6. Die Empfehlungen der guten Praxis (**Art. 8 f.**) sind innovativ, aber rechtsstaatlich bedenklich ausgestaltet und nicht durchdacht (vgl. Beilage). Der EDÖB sollte sie nur genehmigen, nicht selbst erlassen können (mit Rechtsweg); dies hindert ihn nicht daran, eigene "Empfehlungen" zu publizieren, und sie sollten lediglich eine Vermutung der Einhaltung des DSG bewirken.

7. Alle Konkretisierungen der technischen und organisatorischen Massnahmen (**Art. 11**) wie (das heute schon geltende) *Privacy by Design* und (das falsch formulierte) *Privacy by Default* (**Art. 18**) und Dokumentationspflichten sind als solche und eben dort aufzuführen. Die Dokumentationspflicht (**Art. 19**) ist risikobasiert auszugestalten. Es muss verhindert werden, dass die Mittel für den Datenschutz primär in "Bürokratie"-Massnahmen ohne Mehrwert investiert werden. Dies würde der Vorentwurf bewirken; seine praktischen Konsequenzen sind (mangels Praxiserfahrung) nicht zu Ende gedacht.

8. Die Regelung über Daten von verstorbenen Personen (**Art. 12**) gehört nicht ins DSG und macht auch inhaltlich keinen Sinn.

9. Die Informationspflichten (**Art. 13 f.**) sind praxisfern und werden in der gegenwärtigen Ausgestaltung entweder nicht eingehalten werden oder zu einer Informationsüberflutung ohne Mehrwert führen. Die Vorstellung, auf durch solche Informationen für mehr Datenschutz zu sorgen, ist irrig. Nicht ohne Grund wollte daher die deutsche Bundesregierung in ihrem Anpassungsgesetz zur DSGVO die dort ähnlich geregelte Informationspflicht abzuschwächen. Da aufgrund der Konvention auf eine Regelung mit gewissen Pflichtinformationen nicht verzichtet werden kann, ist sie praxistauglich auszugestalten, etwa indem es genügt, dass ein Unternehmen der Informationspflicht über eine Website oder dergl. hinreichend nachkommen kann, ohne aktiv auf die betroffene Person mit den Pflichtinformationen zugehen zu müssen. So kann sie derjenige, der sich dafür wirklich interessiert, im nötigen Detail anschauen. Das entspricht der heutigen Praxis des EDÖB (vgl. Moneyhouse-Entscheid); für die darüber hinaus nötige Transparenz sorgt bereits Art. 4. Die Einschränkung der Information muss bei überwiegendem privaten oder öffentlichem Interesse oder gesetzlich geregelter Datenbearbeitung ohne Restriktion möglich sein.

10. Die Anhörungspflicht bei automatisierten Einzelentscheidungen sind auf Entscheide mit wirklich gewichtigen Konsequenzen einzuschränken (**Art. 15**), für welche kein anderes Korrektiv vorgesehen ist. Es kann nicht sein, dass jeder noch so harmlose Kauf in einem Online-Shop unter

diese Regelung fällt, nur weil der Vertrag durch einen Computer geschlossen wird. Einschränkungen müssen nach den üblichen Rechtfertigungsgründen gelten.

11. Die Pflicht zur formalisierten Datenschutzfolge-Abschätzungen (**Art. 16**) sind auf Bearbeitungen von einer gewissen Dauer und mit wirklich gewichtigen Konsequenzen zu beschränken. Eine Meldepflicht sollte, wenn überhaupt, nur für Fälle vorgesehen werden, wo keine Massnahmen zur Begrenzung der Risiken auf ein vernünftiges Mass möglich und viele Personen betroffenen sind. Nur in solchen Fällen ist es auch angezeigt, dass der EDÖB den Fall näher prüft. Wo ein Unternehmen einen betrieblichen Datenschutzbeauftragten hat, sollte auf Meldungen generell verzichtet werden können (nicht nur in Art. 16).

12. Die *Data Breach Notifications* (**Art. 17**) sollten nicht nur auf eigentliche *Data Breaches* (analog der DSGVO) beschränkt werden, sondern zudem auf Fälle, die eine Vielzahl von Personen betreffen. In allen anderen Fällen ist kein Mehrwert zu erkennen, der den enormen Aufwand rechtfertigt.

13. Die Weitermeldepflicht (**Art. 19**) macht nur Sinn, wenn die betroffene Person es bezüglich eines konkreten Falls, an welchem sie ein überwiegendes, berechtigtes Interesse hat.

14. Das Auskunftsrecht (**Art. 20 f.**) lässt jede wirksame Massnahme gegen dessen heute grassierenden Missbrauch vermissen. Es muss die Möglichkeit der Kostenpflicht eingeführt werden, betont werden, dass nur Daten, nicht Dokumente verlangt werden können (vgl. Entscheid auch des EuGH) und die Möglichkeit vorsehen, zur Missbrauchsbekämpfung Auskunft über einen Dritten zu erteilen (vgl. die Erläuterungen in der Beilage). Vor allem aber muss es möglich sein, überwiegende private und öffentliche Interesse ohne Einschränkung geltend zu machen. Die wichtigsten Fälle (vgl. Beilage) sollten exemplarisch aufgezählt werden. Ferner ist das Auskunftsrecht bezüglich Entscheid zu streichen; die nötigen Informationen können im Rahmen einer Anhörung betr. Einzelfallentscheide zugänglich gemacht werden.

15. Ein Profiling ohne ausdrückliche Einwilligung ist nicht per se eine Persönlichkeitsverletzung (**Art. 23**). Das ist eine unverhältnismässige Regelung.

16. Ein überwiegendes privates Interesse ist in den Fällen von **Art. 24** nicht nur *möglicherweise* sondern *in der Regel* gegeben. Es ist die heutige Formulierung zu verwenden. Der Rechtfertigungsgrund des Vertragsschlusses ist auf am Vertrag interessierte Personen auszudehnen, die Durchsetzung von Rechtsansprüchen vor Gericht als neuen Anwendungsfall analog zu Art. 6 aufzunehmen.

17. Es muss möglich sein, vorsorgliche Massnahmen des EDÖB mit aufschiebender Wirkung anzufechten (**Art. 42 ff.**). Es ist kein Verlass darauf, dass Anordnungen des EDÖB die nötige Zurückhaltung zur Vermeidung von Schaden seitens eines Datenbearbeiters aufweisen werden.

18. Die Strafbestimmungen (**Art. 50 ff.**) sind zu streichen. Es ist ein sinnvolleres, auf die Unternehmen und nicht Einzelpersonen ausgerichtetes Sanktionssystem zu schaffen. Eine vom EDÖB unabhängige Kommission (aber nicht die Kantone) sollte Verwaltungssanktionen aussprechen. Sanktionen für fahrlässige Verstösse sind nicht angezeigt; es sollten nur die schweren und mutwilligen Verstösse gegen klares Recht durch entsprechende Bussen sanktioniert werden. Es ist zu beachten, dass weder bisher noch in Zukunft irgendjemand das DSG je vollständig einhalten

wird, auch der EDÖB nicht. Dem ist Rechnung zu tragen. Zu sanktionieren sind materiell rechtswidrige Datenbearbeitungen, nicht das Unterlassen von flankierenden Massnahmen. Ansonsten werden Datenbearbeiter sich primär auf die "Bürokratie" fokussieren, weil dort Bussen drohen, obwohl sie dem Datenschutz den geringsten Mehrwert verschafft.

19. Die Regel zur beruflichen Schweigepflicht (**Art. 52**) ist in der bisherigen Form beizubehalten. Es gibt keinen Grund für eine Ausdehnung auf praktisch alle Berufstätige.

20. Die Übergangsfrist muss für alle Regelungen zwei Jahre betragen (**Art. 59**).

21. Die Kostenlosigkeit von Verfahren (**ZPO**) ist zu streichen. Sie belastet primär die Staatskasse, wird aber die Durchsetzung von Ansprüchen nicht erleichtern.

22. Jedes *Swiss Finish* gegenüber der DSGVO ist zu vermeiden. Gerade viele grössere Unternehmen werden sich auf die DSGVO ausrichten. Ihre Compliance muss genügen, um auch das künftige DSG einzuhalten.

Gerne stehe ich für weitere Erläuterungen zur Verfügung.

Freundliche Grüsse

David Rosenthal

Beilage

www.jusletter.ch

David Rosenthal

# Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet

Mit mehr als drei Monaten Verspätung präsentierte der Bundesrat am 21. Dezember 2016 den Vorentwurf für ein totalrevidiertes Datenschutzgesetz. Vieles, was er bietet, war erwartet worden. Dennoch stösst das «Weihnachtsgeschenk» auf enorme Resonanz. Insbesondere die strafrechtlichen Sanktionen sorgen für heftige Kritik. Doch der Vorentwurf birgt noch ganz anderen Zündstoff, der allerdings erst auf den zweiten und dritten Blick sichtbar wird. Der Beitrag legt diesen offen und beleuchtet, welche Folgen die Regelungen des Vorentwurfs für die Schweizer Wirtschaft hätten. Denn eines wird klar: Es besteht noch erheblicher Nachbesserungsbedarf.

Beitragsarten: Beiträge
Rechtsgebiete: Datenschutz

Zitiervorschlag: David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017

## Inhaltsübersicht



[Rz 1] Viele Experten – so auch der Autor dieses Beitrags – sind der Ansicht, dass das bestehende Datenschutzgesetz (DSG) in der Sache vollauf genügt, selbst in Anbetracht der schnellen technischen Entwicklungen im Bereich der Informationstechnologie. In seiner Durchsetzung ist es wesentlich effizienter und kostengünstiger als es das neue DSG sein wird. Die Frage nach dem Sinn einer Revision des DSG ist jedoch aus zwei Gründen müssig: Erstens wird die revidierte Konvention 108 des Europarats[1], auf welchem schon das bisherige DSG aufbaut, diverse Anpassungen erforderlich machen.[2] Zweitens dominiert nicht nur in Bundesbern die Angst, die Schweiz könnte ihre Anerkennung als Land mit angemessenem Datenschutz durch die EU verlieren, sollte die Schweiz ihr DSG nicht massiv verschärfen. Ein solches Risiko besteht freilich nach der vorliegend vertretenen Auffassung nicht wirklich, und zwar schon gar nicht, wenn die Schweiz die revidierte Konvention 108 umsetzt, welche den freien Datenfluss mit der EU explizit vorsieht. Die Schweiz gibt sich in diesen Dingen viel zu wenig selbstbewusst. Wenn schon die Einhaltung des «Privacy Shield» für Exporte in die USA als ein datenschutzrechtlich angemessener Standard gilt[3], so wäre bereits das heutige Schweizer Recht hinreichend. Die Angst vor der EU ist somit ein schlechter Berater in dieser Sache. Schon gar nicht ist es angezeigt, in einem revidierten DSG über die Anforderungen der EU hinauszugehen.

[Rz 2] Noch bis zum 4. April 2017 ist es möglich, zum Vorentwurf für das revidierte DSG (VE DSG)[4] Stellung zu nehmen. Es ist davon auszugehen, dass die Vernehmlassung ein grosses Echo auslösen wird, was zu begrüssen ist. Das Bundesamt für Justiz dürfte versuchen, eine entspre-

1 Abrufbar unter http://www.coe.int/en/web/data-protection/modernisation-convention108 (bisher nur im Entwurf), Alle Websites zuletzt besucht am 13. Februar 2017.

2 Über deren Sinnhaftigkeit kann zwar gestritten werden, aber als die breitere politische Öffentlichkeit in Bundesbern von der Revision der Konvention Wind bekam, war es bereits zu spät. Zudem wird auch der Europarat von der EU dominiert, welche im Rahmen der Revision ihre Bedürfnisse, wie sie in der DSGVO ihren Niederschlag fanden, zu grossen Teilen durchgedrückt hat.

3 Vgl. etwa http://europa.eu/rapid/press-release_IP-16-2461_de.htm.

4 https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html; eine englische Fassung ist erhältlich unter http://datenrecht.ch/vorentwurf-des-dsg-englische-fassung/.

chende Botschaft auszuarbeiten, die der Bundesrat möglichst noch vor der Sommerpause dieses Jahres dem Parlament unterbreiten müsste. In der Herbstsession würde dann das Geschäft in der Kommission des Erstrates, in der Wintersession im Plenum beraten werden können. Genügt dies, wird der Zweitrat sich in der Frühjahres- und Sommersession damit befassen können und das revidierte DSG im Sommer oder Herbst 2018 verabschiedet werden können. Damit ist ein Inkrafttreten frühestens auf Januar 2019 möglich, also etwas mehr als ein halbes Jahr nach dem Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018, die bekanntlich für eine ganze Reihe von Schweizer Firmen ebenfalls Anwendung findet. Ein solcher Zeitplan würde es erforderlich machen, dass das Bundesamt für Justiz noch während der parlamentarischen Beratung an den Ausführungsverordnungen arbeitet. Inzwischen halten einige einen solchen Fahrplan für viel zu optimistisch.

[Rz 3] Im Folgenden werden die neuen Regelungen des VE DSG erörtert, welche die Privatwirtschaft betreffen. Auf den behördlichen Datenschutz wird hier nicht eingegangen, auch nicht auf die Anpassungen im Zusammenhang mit Schengen. Wie gezeigt werden wird, haben es einige der Bestimmungen in sich, und sie gehen durchaus über das hinaus, was nach der DSGVO erforderlich ist. Ob ein solcher «Swiss Finish» wirklich sinnvoll ist, wird im Rahmen der Vernehmlassung zu klären sein. Vorliegend wird die Ansicht vertreten, dass strengere oder inkompatible Schweizer Alleingänge zweifellos nicht sinnvoll sind. Dies dürfte auch dem gegenwärtigen politischen Trend entsprechen. Es ist somit noch mit einigen Änderungen zu rechnen.

[Rz 4] Dies gilt im Übrigen auch für die sprachliche Ausgestaltung insbesondere der deutschen Fassung des Gesetzes, die gegenüber der französischen deutlich abfällt, die vermutlich Ausgangspunkt der Arbeiten war. Auf diese Punkte wird in diesem Beitrag nicht näher eingegangen. Es wäre aber sinnvoll, auf die Einheitlichkeit der Begrifflichkeiten zu achten. So ist zum Beispiel nicht ersichtlich, warum in Art. 14 VE DSG das eine Mal von einer «Bekanntgabe» von Personendaten die Rede ist und im nächsten Absatz von deren «Übermittlung».

## 1. Geltungsbereich wird eingeschränkt und ausgeweitet

[Rz 5] Die wichtigste Änderung im Geltungsbereich des revidierten DSG war schon vor dem VE DSG klar: Der Schutz juristischer Personen fällt weg. Erfasst sein soll neu nur noch die Bearbeitung von Daten, die sich auf eine bestimmte oder bestimmbare *natürliche* Person beziehen. Das entspricht der Regelung in fast allen Ländern. Die Anpassung wird kaum zu Diskussionen Anlass geben, auch wenn sie weder systemtreu noch wirklich konsequent ist: Nach Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB), welcher durch das DSG konkretisiert wird, geniessen auch juristische Personen Persönlichkeitsschutz, und sie tun es weiterhin; Art. 13 der Bundesverfassung (BV) gewährleistet den Schutz der Persönlichkeit auch von juristischen Personen. Eine Verletzung durch die Bearbeitung von Personendaten von juristischen Personen ist also über diesen Umweg nach wie vor möglich, wenngleich die Fälle eher selten sein werden.[5] Der Vorteil der Streichung wird sein, dass die formalen Vorschriften betreffend Daten über Firmen wegfallen. Dies wird etwa dem Schindluder mit dem Auskunftsrecht nach dem heutigen Art. 8 DSG (Art.

[5] Das DSG wird hierbei vermutlich analog beigezogen werden. Werden also Daten einer Firma zweckwidrig verwendet, kann argumentiert werden, dass dies Art. 28 ZGB verletzt, weil ein solches Verhalten gemäss DSG eine Persönlichkeitsverletzung darstellt.

20 VE DSG) bei Unterlagen betreffend juristische Personen Einhalt bieten; das Auskunftsrecht dient heute primär der Beschaffung von Beweismitteln für Prozesse und anderen, datenschutzfremden Zwecken, was aber durch die bisherige Gerichtspraxis leider ohne Not geschützt wird.[6] Allerdings darf die Wirkung der Streichung des Schutzes juristischer Personen nicht überbewertet werden: Unternehmen handeln regelmässig durch ihre Organe und Hilfspersonen, und deren Personendaten sind weiterhin durch das DSG erfasst und zwar auch im professionellen Kontext.[7]

[Rz 6] Geht es um Daten natürlicher Personen, wird dem Auskunftsrecht mit dem VE DSG allerdings eine noch grössere Bühne bereitet als bisher: Das DSG soll künftig – ausser für die Gerichte selbst[8] – selbst im Rahmen bereits hängiger Zivilprozesse und laufender Strafverfahren gelten. Somit kann neu selbst während solchen Verfahren weiterhin das Auskunftsrecht zur Beweisbeschaffung benutzt werden, was für eine betroffene Person zweifellos attraktiv ist, da für diese Form der Beweisbeschaffung weder etwas bezahlt werden muss, noch sonst die hohen Hürden der Zivilprozessordnung für Editionsbegehren gelten. Der Missbrauch ist damit leider vorprogrammiert und dürfte mangels sinnvoller Anpassung des Auskunftsrechts in Art. 20 f. VE DSG (vgl. Rz 54 ff., hinten) von den Gerichten weiterhin geschützt werden.

[Rz 7] Der Vorentwurf ändert nicht nur den Geltungsbereich, sondern auch die Begrifflichkeiten in einigen Bereichen. Die gewichtigste Anpassung dürfte die Abschaffung der «Persönlichkeitsprofile» und deren Ersatz durch den Begriff des «Profiling» sein. Dieser umfasst nach Art. 3 Bst. f VE DSG «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 extrem breit, und die Schweiz geht damit deutlich über die entsprechende Regelung der EU hinaus. Anders als in der DSGVO ist auch das Profiling von Hand erfasst, also beispielsweise das Ausfüllen einer Mitarbeiterbeurteilung oder die Einschätzung eines Arztes, wie sich die Krankheit einer Person entwickeln wird. Aber auch die Versicherung, die im Rahmen einer Police ein Alterskapital berechnet, nimmt nach dem Wortlaut der VE DSG ein Profiling vor, da sie eine Entwicklung bezüglich wirtschaftlicher Lage des Versicherten prognostiziert. Dies alles gilt neu nach Art. 23 Abs. 2 Bst. d VE DSG *per se* als Persönlichkeitsverletzung, was wiederum einen Rechtfertigungsgrund erfordert, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden ist. Eine solche Regelung erscheint doch etwas übertrieben.

[Rz 8] Ob für das Profiling Personendaten benutzt werden oder nicht, spielt zudem keine Rolle («Daten oder Personendaten»). Die Befürchtung, dass damit auch das Bearbeiten von nicht personenbezogenen Daten plötzlich erfasst wäre, dürfte zwar unberechtigt sein: Hier greift Art. 2 Abs. 1 VE DSG, wonach das DSG nur dann gilt, wenn Personendaten bearbeitet werden. Ein Profiling ist somit dann erfasst, wenn sich mindestens das Ergebnis auf eine bestimmte oder bestimmbare Person bezieht. Die Formulierung «Daten oder Personendaten» ist trotzdem unnötig

---

6 Vgl. statt vieler BGE 138 III 425 und Urteil des Bundesgerichts 4A_506/2014 vom 3. Juli 2015; vgl. auch David Rosenthal, Aktuelle Anwaltspraxis 2013, S. 731 ff.; ders., Aktuelle Anwaltspraxis 2015, S. 586 ff.

7 Hierbei ist auf Erwägung 14 der DSGVO hinzuweisen, die erklärt, dass die DSGVO keine Anwendung finden soll auf die Kontaktdaten juristischer Personen, was häufig natürliche Personen sind. Die Tragweite dieser Erklärung ist allerdings nicht klar. Es gibt etliche Daten natürlicher Personen in ihrer Eigenschaft als Arbeitnehmer einer juristischen Person, die ohne Weiteres schutzwürdig sind.

8 Der VE DSG regelt nur noch die eidgenössischen Gerichte; die Datenbearbeitung der kantonalen Gerichte wird von den kantonalen Datenschutzgesetzen geregelt werden müssen. Allerdings ist die diesbezügliche Regelung in Art. 57 VE DSG mit Bezug auf Art. 2 Abs. 3 VE DSG nicht korrekt formuliert. Es fehlt der Hinweis, dass die Regelungen für eidgenössische Gerichte im kantonalen Recht sinngemäss für kantonale Gerichte umzusetzen ist.

und irreführend: Handelt es sich beim Output eines Profilings um Personendaten, muss es sich naturgemäss auch beim Input um solche handeln, weil ein Personenbezug offenkundig möglich ist, wie das Profiling selbst beweist. Der Hinweis auf «Daten» ist daher zu streichen.

[Rz 9] Der Katalog der besonders schützenswerten Personendaten wurde wie von der revidierten Konvention 108 vorgegeben um genetische und biometrische Daten erweitert, letztere mit der Einschränkung, dass nur Daten gemeint sind, die eine natürliche Person eindeutig identifizieren. Diese Beschränkung ist allerdings wenig hilfreich: Jedes Gesichtsfoto soll nach dem Vorentwurf künftig als besonders schützenswertes Personendatum gelten. Gedacht war die Regelung an sich etwas enger: Gemäss dem Erläuterungsbericht sollen nur jene Fotos erfasst sein, die mit spezifischen technischen Mittel so bearbeitet wurden, dass eine eindeutige Identifizierung oder Authentisierung eines Individuums möglich ist. Gemeint sind also Fälle der Gesichtserkennung, wobei die meisten Fälle wiederum aufgrund fehlender Zuverlässigkeit in der Erkennung wegfallen dürften. Hier besteht somit noch Nachbesserungsbedarf in der Legaldefinition. Erfasst sein sollten nach Art. 3 Bst. c Ziff. 4 VE DSG nicht jene biometrische Daten, die eine natürliche Person eindeutig identifizieren, sondern nur solche, die zum Zweck bearbeitet werden, dies zu tun. Mehr verlangt auch die Konvention 108 nicht. Bilder in der Zeitung, auf welchen Personen zu erkennen sind, wären nach dieser Definition somit nicht mehr besonders schützenswerte Personendaten, während dies gemäss Vorentwurf noch so wäre.

[Rz 10] Weggefallen ist auch das Konzept der Inhaberschaft einer Datensammlung. Es wurde ersetzt durch den in der EU schon seit langem gebräuchlichen Begriff des «Verantwortlichen» (*Controller*) und des «Auftragsbearbeiters» (*Processor*). Die Definition des Verantwortlichen gibt aber nicht ganz das in Europa herrschende Begriffsverständnis wieder: Der Verantwortliche zeichnet sich nicht dadurch aus, dass er über Zweck, Mittel und Umfang der Bearbeitung der Daten entscheidet, sondern dass er dies *final* tut oder tun kann, also der «Herr der Daten» ist. In der Praxis wird der Entscheid über die Mittel und den Umfang der Datenbearbeitung häufig dem Auftragsbearbeiter delegiert, wie z.B. auch die Bestimmung der angemessenen Schutzmassnahmen. In den Erläuterungen wird ohne Begründung vertreten, dass die Arbeitnehmer eines Verantwortlichen nicht als Auftragsbearbeiter gelten, was systematisch und dogmatisch falsch ist. Die Regeln der Auftragsbearbeitung müssen auch im Verhältnis zu den eigenen Arbeitnehmern gelten, denen ein Unternehmen die Bearbeitung von Daten anvertraut, auch wenn die Genehmigung nach Art. 7 Abs. 3 VE DSG regelmässig implizit als erteilt gelten wird und die Information nach Art. 13 Abs. 4 VE DSG für diese Fälle keinen Sinn macht. Diese beiden Neuerungen sollten daher relativiert werden.

[Rz 11] Anpassungsbedarf besteht ferner bezüglich der Verantwortlichkeiten des Auftragsbearbeiters: Zahlreiche der neuen Bestimmungen nehmen nicht nur den Verantwortlichen in die Pflicht, sondern parallel auch den Auftragsbearbeiter. Dieser wird jedoch oftmals gar nicht in der Lage sein, aus eigenem Antrieb oder in eigener Verantwortlichkeit diesen Pflichten nachzukommen; in der DSGVO werden die Auftragsbearbeiter nicht derart in die Pflicht genommen. Beispiele hierfür sind die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 16 VE DSG), *Privacy by Design* und *Privacy by Default* (Art. 18 VE DSG) oder die Information von Datenempfängern über etwaige Berichtungen oder Löschungen von Daten (Art. 19 VE DSG). Für all diese Aufgaben kann sinnvollerweise nur der Verantwortliche verantwortlich sein, auch wenn er zu deren Umsetzung allenfalls die Hilfe eines Auftragsbearbeiters beanspruchen wird.

[Rz 12] Der Begriff der Datensammlung selbst soll im revidierten DSG ebenfalls weggefallen. Dogmatisch und systematisch war das Konzept der Inhaberschaft sauberer und differenzierter

als die neue Lösung, aber sie war seit je her selbst für Spezialisten schwer zu verstehen. Die Anpassung erscheint als Massnahme zur Harmonisierung mit den internationalen Gepflogenheiten im Datenschutzrecht daher sinnvoll. Sie hat immerhin die Folge, dass diverse Pflichten ausgeweitet werden: Das Auskunftsrecht nach Art. 8 DSG galt bisher nur für Daten in Datensammlungen; neu soll es jedenfalls nach dem Wortlaut für alle Daten, die ein Verantwortlicher bearbeitet, gelten (Art. 20 Abs. 1 VE DSG). Sinngemäss wird es freilich weiterhin nur für jene Daten zur Anwendung kommen können, die nach der betroffenen Person erschlossen werden können, denn wenn ein Verantwortlicher selbst nicht ohne Weiteres nach einer bestimmten Person in seinem Datenbestand suchen kann, weil es für seine Datenbearbeitung keine Rolle spielt, wird dies von ihm auch im Rahmen des Auskunftsrechts nicht verlangt werden können. Anwendungsfälle, wo sich der Unterschied zeigt, könnten zum Beispiel Aufnahmen von Sicherheitskameras sein: Sie sind regelmässig keine Datensammlung, da sie nicht nach betroffenen Personen erschlossen werden können. Gibt eine Person unter neuem Recht an, wann sie von einer Kamera erfasst wurde und will sie die Aufnahme sehen, wird ihr dieser Zugang unter neuem Recht gewährt werden müssen. Die praktische Relevanz ist in diesem Falle allerdings beschränkt: Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) stellt sich aufgrund des gefühlten Datenschutzes und ohne Rechtsgrundlage auf den Standpunkt, dass schon unter heutigem Recht eine Auskunftspflicht besteht, und kaum jemand wagte es bisher, ihm zu widersprechen.

## 2. Kein Methodenwechsel bei «Personendaten»

[Rz 13] Vom Wegfall des Schutzes juristischer Personen abgesehen, soll der Begriff der Personendaten auch im neuen Recht so bleiben, wie er ist[9]. Dies war ein mit Spannung erwarteter Punkt und der Entscheid ist richtig und wichtig. Es bleibt somit bei durch die bundesgerichtliche Rechtsprechung bestätigten «relativen» Methode, wenn es darum geht zu ermitteln, ob die betroffene Person bestimmbar ist. Danach genügt es nicht, dass der Aufwand zur Identifizierung objektiv gering genug ist, dass ein Interessent ihn nach allgemeiner Lebenserfahrung auf sich nimmt (objektive Komponente). Wesentlich ist ebenso, welches Interesse der Datenbearbeiter oder ein Dritter mit Zugang zu den Daten an der Identifizierung hat (subjektive Komponente), was vom konkreten Fall abhängig ist.[10] Es genügt daher nicht wie bei der «absoluten» Methode, dass irgendjemandem die Identifizierung möglich ist. Obwohl in der EU immer wieder die «absolute» Methode vertreten wird, hat der EuGH kürzlich auch für das geltende EU-Recht die relative Methode bestätigt.[11]

[Rz 14] Daran dürfte sich auch unter der DSGVO bei richtiger Auslegung nichts ändern. Zwar wird im Falle der DSGVO teilweise vertreten, dass bereits dann Personendaten vorliegen, wenn sie eine «Singularisierung» erlauben, also so spezifisch sind, dass sie sich nur noch auf eine bestimmte Person beziehen können, selbst wenn sich diese nicht identifizieren lässt. Dies übersieht

9 Erläuterungen VE DSG, S. 43.

10 BGE 136 II 508, E. 3.2.

11 Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Breyer*, welches die Frage der Identifikation des Inhabers einer IP-Adresse zum Inhalt hatte. Während die Bestimmbarkeit der betroffenen Person für den Internet-Service-Provider klar war (RN 33 f., mit Hinweis auf den Urteil des EuGH vom 24. November 2011 C-70/10 *Scarlet Extended*), war sie gemäss EuGH für den Betreiber einer Website, der die IP-Adresse für den Fall von Cyberangriffen aufzeichnete, separat zu prüfen (RN 44–49). Damit folgte der EuGH wie schon zuvor BGE 136 II 508 auch für das EU-Recht der «relativen» Methode.

jedoch, dass die DSGVO die Singularisierung nur als Indiz für eine Identifizierbarkeit vorsieht[12] und sie als Konzept über massive Mängel verfügt, die sie untauglich werden lassen.[13] Wesentlich zuverlässiger ist hierbei der sog. Referenzdaten-Test, wie ihn auch der EuGH angewandt hat.[14]

[Rz 15] Das Festhalten am bisherigen Begriff des Personendatums im Vorentwurf bedeutet insbesondere, dass die Bekanntgabe von pseudonymisierten Daten an Personenkreise, die nicht über den Schlüssel zur Zuordnung der Daten zu betroffenen Personen verfügen, weiterhin *keine* Bekanntgabe von Personendaten darstellen wird und daher auch die diesbezüglichen datenschutzrechtlichen Kautelen nicht beachtet werden müssen. Dies gilt jedenfalls solange die Nichtidentifizierbarkeit der Daten durch die Dritten sichergestellt ist. Das macht auch Sinn. Wäre dem nämlich nicht so, wäre beispielsweise die Bekanntgabe von geschwärzten Unterlagen durch Behörden oder Unternehmen an vielen Orten nicht mehr zulässig, ebenso nicht die Speicherung von vollverschlüsselten Daten auf einem Speichersystem im Internet. Beides sind letztlich Formen der Pseudonymisierung.

## 3. Bisheriges Regelungskonzept mit Bearbeitungsgrundsätzen bleibt

[Rz 16] Das bisherige Regelungskonzept des DSG, welches von einer generellen Erlaubnis zur Bearbeitung von Personendaten ausgeht und einzelne Fälle definiert, in welchen sie verboten ist, soll bestehen blieben. Es gilt im privaten Bereich somit weiterhin das Prinzip des «opt-out», nicht des «opt-in». Eine Zustimmung zur Bearbeitung von Personendaten ist weiterhin nicht zwingend; anders als in der DSGVO soll es in der Schweiz nicht erforderlich sein, für eine Datenbearbeitung einen Rechtfertigungsgrund vorweisen zu können.[15] Ein Rechtfertigungsgrund wird nur und erst dann benötigt, wenn eine Datenbearbeitung die Persönlichkeit einer betroffenen Person verletzt, was sich neu aus Art. 24 VE DSG ergibt. In welchen Fällen eine Persönlichkeitsverletzung vorliegt, umschreibt Art. 23 VE DSG, welcher gegenüber dem heutigen Art. 12 DSG erweitert wurde.

[Rz 17] Aber auch hier bleibt das Grundkonzept dasselbe: In Art. 23 Abs. 2 VE DSG wird aufgezählt, in welchen Fällen eine Persönlichkeitsverletzung *per se* vorliegt, nämlich bei Verletzung der Bearbeitungsgrundsätze, bei einer Datenbearbeitung gegen den erklärten Willen einer betroffenen Person (wie bisher), bei der Bekanntgabe von besonders schützenswerten Personendaten an Dritte (wie bisher) und beim Profiling ohne ausdrückliche Einwilligung der betroffenen Person.

---

12 Erwägung 26 der DSGVO («To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, . . . »).

13 Beispielsweise wäre ein automatisches Foto einer Person in einer misslichen Lage aufgrund der Einmaligkeit der Aufnahme selbst dann ein Personendatum, wenn ausser dieser Person selbst kein Mensch auf der Welt herausfinden kann, um wen es sich handelt.

14 Hierbei wird geprüft, ob die bearbeiteten Daten bereits verfügbaren oder nach allgemeinem Ermessen wahrscheinlich verfügbaren Daten real existierender Personen eindeutig zugeordnet werden können. Können aus biologischem Material beispielsweise genetische Daten gewonnen werden, so werden diese erst dann zu Personendaten, wenn diese mit Referenzdaten realer, bekannter Personen abgeglichen werden können, wobei solche Referenzdaten oder Vergleichsproben normalerweise nicht verfügbar sein werden (vgl. Botschaft Humanforschungsgesetz, BB 2009 8045, 8096). Denselben Test wendete auch das Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Breyer* an, um festzustellen, ob eine IP-Adressen für einen Website-Provider Personendaten darstellen, was es im konkreten Fall bejahte, da er davon ausging, dass er Zugang zu den Referenzdaten des Internet-Service-Providers erlangen würde. Die Frage der Zugänglichkeit zu Referenzdaten ist jeweils aus der Perspektive derjenigen zu beurteilen, die Zugang zu den bearbeiteten Personendaten haben («relative Methode»).

15 Vgl. Art. 6 DSGVO.

Letztere Regelung ist neu und insofern nicht ganz nachvollziehbar, als dass der Begriff des Profiling extrem breit definiert ist. Dies wird zweifellos noch für Diskussionen sorgen.

[Rz 18] Art. 23 Abs. 2 Bst. a VE DSG führt neu auch Art. 5 und 6 VE DSG auf, welche sich auf die Bekanntgabe ins Ausland beziehen. Dies ist lediglich eine redaktionelle Klarstellung, denn schon bisher war eine unerlaubte Bekanntgabe ins Ausland als Persönlichkeitsverletzung zu werten. Die Aufzählung von Art. 5 und 6 VE DSG in Art. 23 VE DSG ändert allerdings nichts daran, dass die Rechtfertigungsgründe in Art. 24 VE DSG, insbesondere der Rechtfertigungsgrund des überwiegenden privaten Interesses, in den Fällen von Art. 5 und 6 VE DSG keine Anwendung finden.

[Rz 19] Hinzuweisen ist in diesem Zusammenhang allerdings auf einen Fehler in den Erläuterungen: Diesen zufolge kommt Art. 23 Abs. 3 VE DSG (er handelt von veröffentlichten Daten) angeblich nur zum Tragen, wenn die Bearbeitung von Daten rechtmässig erfolge, d.h. die Grundsätze von Art. 4, 5, 6 und 11 eingehalten würde.[16] Das ist falsch. Abs. 3 führt dazu, dass die Bearbeitung von Daten, die mit Wissen und Willen einer Person publiziert wurden, in der Regel selbst dann rechtmässig ist, wenn sie unter Verletzung der Bearbeitungsgrundsätze erfolgt. Das war schon im bisherigen Recht so.

[Rz 20] Die exemplarische Aufzählung der Fälle, in welchen von einem überwiegenden Interesse auszugehen ist, wurde überarbeitet. Sie entsprechend im Kern der heutigen Regelung von Art. 13 Abs. 2 DSG, mit gewissen geringfügigen Anpassungen:

- Der Rechtfertigungsgrund der Kreditüberprüfung soll nur noch gelten, wenn die betroffene Person volljährig ist, was zwar auf den ersten Blick zum Schutz von Kindern einleuchten mag, aber bei näherer Betrachtung nicht sinnvoll erscheinen: Online-Shops, die auch von nicht volljährigen Kunden genutzt werden, stellen zum Beispiel häufig auf automatisierte Kreditprüfungen ab, in deren Rahmen sie auch erfahren, ob eine Person bereits volljährig ist oder nicht. Auf diese Datenquelle würde verzichtet werden müssen. Nicht volljährige Personen werden notabene mindestens bei gewissen Kreditauskunfteien zwar als solche ausgewiesen, erhalten aber automatisch ein positives Kreditrating. Diese Daten dürfen neu möglicherweise nicht mehr bereitgehalten werden. Weiterhin nicht bearbeitet werden dürfen auch besonders schützenswerte Personendaten, was in jenen Fällen als problematisch erscheint, als dass es sich um Daten zu Verurteilungen im Zusammenhang mit bestimmten Vermögensdelikten handelt, die durchaus von erheblicher Relevanz für die Kreditwürdigkeit einer Person sind.
- Der Rechtfertigungsgrund der nicht-personenbezogenen Bearbeitung erfordert nun nicht mehr nur, dass die Ergebnisse so veröffentlicht werden, dass keine Rückschlüsse auf die betroffenen Personen mehr möglich sind. Auch vorgängig darf Dritten nichts bekanntgegeben werden, was aus deren Sicht Personendaten sind. Sie müssen somit pseudonymisiert oder anonymisiert werden. Zudem wird in Erinnerung gerufen, dass Personendaten anonymisiert werden müssen, sobald es der Zweck der Bearbeitung erlaubt. Das ergab sich allerdings schon bisher aus dem Grundsatz der Verhältnismässigkeit.

[Rz 21] Die Formulierung von Art. 24 Abs. 2 VE DSG ist insofern zurückhaltender geworden, als dass nun davon die Rede ist, dass in den aufgeführten Fällen das überwiegende private Interesse nur noch «möglicherweise» gegeben ist. Gemäss den Erläuterungen soll dies darauf hinwirken,

16 Erläuterungen VE DSG, S. 69.

dass die spezifischen Umstände des Einzelfalls stärker berücksichtigt werden.[17] Für diese Einschränkung gibt es jedoch keinen Grund; die bisherige Regelung und Formulierung hat sich bestens bewährt. Durch die Einführung des Worts «möglicherweise» wird nunmehr die Rechtssicherheit, welche mit Art. 23 Abs. 2 VE DSG geschaffen werden soll, gleich wieder zunichtegemacht. Schon die bisherige Regelung galt nicht absolut, aber sie stellte klar: Gibt es keine gewichtigen Gründe von der Bewertung in Art. 13 Abs. 2 DSG abzuweichen, wird das überwiegende Interesse nach Ansicht des Gesetzgebers gegeben sein. Zu Problemen führte dieses System bisher nicht; dazu sind die aufgezählten Fälle zu klar.

[Rz 22] Die Bearbeitungsgrundsätze wurden im VE DSG sinnvollerweise in Art. 4 zusammengefasst. Es sind jedenfalls auf den ersten Blick keine grundlegenden Änderungen ersichtlich. Der Grundsatz der Zweckbindung und Erkennbarkeit wurde in Art. 4 Abs. 3 VE DSG zusammengefasst. Bisher genügte es für die Zweckbindung, dass eine bestimmte Bearbeitung vom Schweizer Recht vorgeschrieben war. Nach dem neuen Wortlaut und System scheint das nicht mehr der Fall zu sein. Dies würde bedeuten, dass Unternehmen auch auf gesetzlich vorgeschriebene Datenbearbeitungen hinweisen müssen, was wenig sinnvoll erscheint. Dieser Punkt bedarf der Klärung mindestens in den Erläuterungen, wonach die Tatsache, dass eine Bearbeitung gesetzlich vorgesehen ist, diese zugleich auch erkennbar macht.

[Rz 23] Das in Abs. 3 neu eingefügte Erfordernis der «klaren» Erkennbarkeit ist hingegen ersatzlos zu streichen: Es ist nicht ersichtlich, welchen Mehrwert dieser Zusatz hat; eine materielle Änderung gegenüber der heutigen Rechtslage ist erklärtermassen nicht beabsichtigt.[18] Die Deutlichkeit, mit welcher auf einen bestimmten Bearbeitungszweck hinzuweisen ist, ergibt sich schon unter dem heutigen Recht aus dem Risiko, dass mit ihm für die betroffene Person verbunden ist. Es gibt keinen Grund, daran etwas zu ändern. Das Wort «klar» im Zusammenhang mit der Erkennbarkeit des Bearbeitungszwecks sorgt lediglich für Verwirrung.

[Rz 24] Zu begrüssen ist hingegen die Einführung «kompatibler» Bearbeitungszwecke. Nach Art. 4 Abs. 3 Satz 2 VE DSG ist neu die Bearbeitung von Daten auch zu Zwecken erlaubt, die zwar nicht erkennbar, mit den erkennbaren Zwecken aber «vereinbar» sind. Damit greift die Formulierung ein Konzept auf, welches das EU-Recht bereits kennt und in der Praxis gewisse Erleichterungen mit sich bringt.[19] Ein typisches Beispiel ist die Anonymisierung von zu einem Zweck A beschafften Personendaten, um sie für den Zweck B zu verwenden. Der Vorgang der Anonymisierung ist eine Datenbearbeitung, die ihrerseits dem Zweckbindungsgrundsatz unterliegt. Ist dieser Zweck B nicht von Anfang an erkennbar gewesen, verlangt seine Verfolgung an sich einen Rechtfertigungsgrund. Das ist neu nicht mehr der Fall.

[Rz 25] Ein weiteres Praxisbeispiel ist die Beschaffung von Kundendaten zwecks Abwicklung von Verträgen. Will das Unternehmen diese Daten auch für eigene Targeting-, Analyse- oder Marketingzwecke verwenden und hat es dies im Rahmen der Datenbeschaffung nicht angekündigt, so stellt sich unter heutigem Recht die Frage, ob diese Nutzungen mindestens aus den Umständen ersichtlich waren. Ist dem (ausnahmsweise) nicht so, wäre ein Rechtfertigungsgrund erforderlich. Neu entfällt dieses Erfordernis: Beide Nutzungen dürften zwar vom ursprünglichen Be-

17 Erläuterungen VE DSG, S. 69.

18 Erläuterungen VE DSG, S. 46.

19 Art. 6 Abs. 4 DSGVO.

schaffungszweck nicht abgedeckt, mindestens aber mit diesem «vereinbar» sein.[20] Nicht richtig ist allerdings die Aussage in den Erläuterungen, dass eine Weiterbearbeitung dann als vereinbar gilt, wenn sie durch einen Rechtfertigungsgrund wie etwa eine Einwilligung des Betroffenen legitimiert ist;[21] hierbei werden zwei verschiedene Konzepte unzulässigerweise miteinander vermischt. Ob ein neuer Datenbearbeitungzweck mit dem ursprünglichen Zweck vereinbar ist, ergibt sich aus einer inhaltlichen Verwandtschaft, den möglichen Auswirkungen der Datenbearbeitung zum neuen Zweck, vorhandenen Massnahmen zum Schutz der betroffenen Person oder ihrem Verhältnis zum Verantwortlichen.

[Rz 26] Nur scheinbar neu ist der Grundsatz in Art. 4 Abs. 4 VE DSG, welcher eine Anonymisierung von Daten verlangt, sobald der Zweck der Bearbeitung dies erlaubt. In Tat und Wahrheit ergab sich dies schon bisher aus dem Grundsatz der Verhältnismässigkeit, der weiterhin gilt[22]. Neu formuliert wurde auch der Grundsatz der Datenrichtigkeit in Art. 4 Abs. 5 VE DSG, dessen neuer Wortlaut etwas absoluter abgefasst ist, als bisher. Da eine Änderung des bisherigen Rechts nicht beabsichtigt ist,[23] stellt sich allerdings die Frage, warum der Wortlaut angepasst wird; die bisherige Formulierung erscheint sachgerechter.

[Rz 27] Die Verletzung der Bearbeitungsgrundsätze in Art. 4 VE DSG wird notabene weiterhin nicht sanktioniert.

## 4. Einwilligung: Alles bleibt beim Alten

[Rz 28] Die Einwilligung schien bisher das Allerheilmittel im Datenschutz zu sein, geht es doch letztlich um informationelle Selbstbestimmung. Die Anpassungen der DSGVO in diesem Bereich liessen allerdings Böses erahnen. Auch hier haben sich die Befürchtungen nicht bewahrheitet: Der Wortlaut der Definition der Einwilligung in Art. 4 Abs. 6 VE DSG wurde zwar um den Hinweis erweitert, dass eine Einwilligung eindeutig sein muss, um gültig zu sein. Damit wird jedoch lediglich wiederholt, was heute schon gilt.[24] Es gilt auch im Bereich der Einwilligung weiterhin ein risikobasierter Ansatz: Je einschneidender die Folgen einer Einwilligung, desto klarer muss sie sein. Je ungewöhnlicher die beabsichtigte Datenbearbeitung, desto deutlicher muss darauf hingewiesen werden. Die Erläuterungen sind insofern nicht korrekt, als dass eine Einwilligung nicht den gesamten Zweck einer Bearbeitung abdecken muss[25]; es genügt, dass sie jenen Teil einer Bearbeitung abdeckt, für den sie eingeholt wird.

[Rz 29] Nach Schweizer Recht wird es aber weiterhin möglich sein, dass etwa ein Kästchen auf einem Online-Formular, das eine bestimmte Datenbearbeitung für erlaubt erklärt, standardmässig bereits angekreuzt ist. Dies wird unter der DSGVO mit der Begründung abgelehnt, dass die Einwilligung in Bezug auf diese Bearbeitung nicht mehr eine unmissverständliche sei, was dort be-

20 Erläuterungen VE DSG, S. 46, welche das Versenden von unverlangten Werbe-E-Mails als Beispiel für eine nicht vereinbare Nutzung nennt.

21 Erläuterungen VE DSG, S. 46.

22 Art. 4 Abs. 2 VE DSG.

23 Erläuterungen VE DSG, S. 47.

24 Erläuterungen VE DSG, S. 47.

25 Ebd.

grifflich ebenfalls verlangt wird.[26] Die Begründung verkennt jedoch den Gesamtzusammenhang und stimmt jedenfalls für die Schweiz nicht: Ist das Kästchen in seinem Zustand (angekreuzt oder nicht) Gegenstand einer Erklärung, die ihrerseits einer eindeutigen Willensbekundung der betroffenen Person unterliegt, so gilt dies auch für den Inhalt des Kästchens, und zwar gleichgültig, ob es zunächst angekreuzt war oder nicht. Entscheidend ist der Zustand zum Zeitpunkt der Willenserklärung. Sonst wäre auch jeder Satz, der ganz ohne Wahlmöglichkeit angezeigt wird («Es gelten die AGB und die Preisliste.») nicht von der Willenserklärung erfasst, was wohl niemand behaupten wird und auch den Grundkonzepten des Schweizer Rechts zuwiderlaufen würde. Wenn überhaupt müsste die Frage der Voreinstellung des Kästchens im Rahmen der Regelung zum «*Privacy by Default*» in Art. 18 Abs. 2 VE DSG beantwortet werden (dazu Rz 79 hinten).

[Rz 30] Verwirrend sind die Ausführungen der Erläuterung in Bezug auf die Frage, wann eine Einwilligung eines «ausdrückliche» ist, wie sie für besonders schützenswerte Personendaten und das Profiling erforderlich ist.[27] Hierzu gibt es verschiedene Ansichten, wobei nicht klar ist, worin sich diese wirklich unterscheiden.[28] Zur vermeintlichen Klärung wurden im VE DSG die französischen und italienischen Begriffe «explicite» und «explicito» durch «exprès» und «espresso» ersetzt. Es wird ausgeführt, dass dies auch durch ein Zeichen geschehen kann, wie etwa das Anklicken einer Schaltfläche.[29] Die Frage, wann eine Einwilligung eine ausdrückliche ist, wird damit freilich nicht geklärt.

[Rz 31] Hierzu ist es nötig, das Wesen der Einwilligung in seine Einzelteile zu zerlegen. Leider herrscht auch in der Grundlagenliteratur zum Obligationenrecht bezüglich den verschiedenen Arten der Willenserklärung, wie sie auch jeder Einwilligung zugrunde liegt, ein Wildwuchs.[30] Die meisten Definitions- und Erklärungsversuche erweisen sich bei näherer Betrachtung als nicht zu Ende gedacht oder sogar in sich widersprüchlich. Dabei werden Begriffe wie «ausdrücklich», «konkludent» und «Stillschweigen» beliebig gemischt und gegenübergestellt.[31] So wird teilweise behauptet, die Frage der Ausdrücklichkeit beziehe sich nur auf die Form einer Willenserklärung, was schon begrifflich falsch ist, weil das Gegenstück zur ausdrücklichen Willenserklärung – die konkludente – sich sachlogisch überhaupt nur aus einer inhaltlichen Komponente ergeben kann. Wird nur von der Form einer Willenserklärung gesprochen, so ist zwischen aktivem und passivem Verhalten und den dazu benutzten Elementen wie Sprache, Gestik, Schrift oder sonstigen Bewegungen zu unterscheiden. Ein solches Verhalten muss jedoch immer in einen inhaltlichen Kontext gesetzt werden, um zur Willenserklärung zu werden; auch ein simples «Ja» oder der

---

26 Art. 4 Ziff. 11 DSGVO, Erwägung 32 DSGVO (wonach ein bereits angekreuztes Kästchen dem Stillschweigen gleichgestellt wird).

27 Es stellt sich die Frage, ob es überhaupt in allen vorgesehenen Fällen sinnvoll ist, eine ausdrückliche Einwilligung zu verlangen; gerade der Begriff des Profiling ist so breit angelegt, dass er auch viele nicht sensible Konstellationen erfasst. Dass trotzdem Ausdrücklichkeit verlangt wird, wird rein historische Gründe haben, da sie bisher auch für Persönlichkeitsprofile verlangt wurde.

28 Erläuterungen VE DSG, S. 47, m.w.H.

29 Erläuterungen VE DSG, S. 47 f.

30 Vgl. Alfred Koller, Schweizerisches Obligationenrecht Allgemeiner Teil, § 3, Rn. 127, der von einem «eigentlichen Wirrwarr» spricht.

31 Claire Huguenin, Obligationenrecht Allgemeiner und Besonderer Teil, Rn. 175, stellt der ausdrücklichen Willenserklärung die konkludente gegenüber, wobei die stillschweigende Erklärung als Unterfall der konkludenten und ausnahmsweise auch der ausdrücklichen Willenserklärung erachtet wird. Gl.M. Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 9; Andreas Furrer/Markus Müller-Chen, Obligationenrecht Allgemeiner Teil, Kapitel 2, Rn. 52. Andreas von Tuhr, Allgemeiner Teil des Schweizerischen Obligationenrechts, S. 163, bezeichnet die konkludente Willenserklärung hingegen als Unterfall der stillschweigenden; so auch Max Keller/Christian Schöbi, das Schweizerische Schuldrecht, Band I, S. 32.

Klick auf den «Ich stimme zu»-Knopf auf einer Website sagt für sich nichts aus.[32] Erst aus diesem Zusammenspiel von Form und Inhalt ergibt sich, ob eine Willenserklärung eine ausdrückliche oder – dem Gegenstück – eine konkludente ist.

[Rz 32] Ausdrücklich ist eine Einwilligung in eine Datenbearbeitung korrekterweise dann, wenn ein (i) aktives Verhalten oder ein solches vorliegt, das als affirmativ vereinbart wurde[33], und (ii) die Bedeutung dieses affirmativen Verhaltens sich direkt auf die betreffende Datenbearbeitung bezieht. Nicht ausdrücklich und somit konkludent ist eine Einwilligung in eine Datenbearbeitung dann, wenn das affirmative Verhalten sich lediglich auf eine Handlung bezieht, welche die fragliche Datenbearbeitung zur Folge hat und nicht auf die Datenbearbeitung selbst.

[Rz 33] Ein Beispiel illustriert dies: Wer ein Produkt auf die Ladentheke legt, gibt kund, dass er dieses Produkt kaufen möchte. Dies ergibt sich aus den Umständen. Nimmt die Person die gleiche Handlung zu Hause am Küchentisch vor, würde dies hingegen nicht bedeuten, dass sie das Produkt kaufen möchte; der Wille das Produkt kaufen zu wollen, wird nicht ausdrücklich kundgetan, sondern geht lediglich aus den Umständen hervor. Ausdrücklich ist hierbei höchstens die Tatsache, dass die Sache auf die Theke gelegt worden ist. Wer für den Kauf eines Produkts ein Formular mit seinen Personendaten ausfüllt und dieses einem Vertragspartner übergibt, nimmt ein affirmatives Verhalten vor. Eine lediglich konkludente Einwilligung in Bezug auf die mit dem Kauf zusammenhängende Datenbearbeitung liegt vor, wenn auf dem Formular nur auf den Kauf Bezug genommen wird, auch wenn aus den Umständen (d.h. implizit) hervorgeht, dass der Vertragspartner zur Abwicklung die übergebenen Personendaten bearbeiten wird. Dies ist dementsprechend auch nicht als ausdrückliche, sondern konkludente Einwilligung in eine Datenbearbeitung zu werten.[34] Steht auf dem Formular hingegen (auch), dass die Daten für Marketingzwecke bearbeitet werden, so resultiert aus der Übergabe des Formulars – also der exakt derselben Handlung bzw. Form – eine ausdrückliche Einwilligung bezüglich der Marketingzwecke.[35] Entscheidend ist somit vereinfacht formuliert, ob die Datenbearbeitung, in welche eingewilligt werden soll, beim Namen genannt wird. Dieses Begriffsverständnis wird auch dem Schutzzweck, den das Erfordernis der Ausdrücklichkeit hat, optimal gerecht.

[Rz 34] Eine in der Praxis wichtige Detailfrage ist die Möglichkeit der Einwilligung durch Stillschweigen oder rein passives Verhalten. Hierzu halten die Erläuterungen fest, dass ein passives Verhalten nie eine ausdrückliche Einwilligung sein kann. Das ist nicht richtig. Es ist auch hier zu differenzieren: Stillschweigen ist normalerweise keine Zustimmung, sondern nur unter den Voraussetzungen von Art. 6 des Obligationenrechts (OR). Wenn jedoch zwei Parteien miteinander vereinbart haben, dass Stillschweigen als Zustimmung gilt, dann stellt ein Stillschweigen in der definierten Situation ein affirmatives Verhalten, mithin ein vereinbartes Zeichen der Zustimmung

---

32 So auch Alfred Koller, Schweizerisches Obligationenrecht Allgemeiner Teil, §3, Rn. 116. Vgl. auch Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 7.

33 Es wurde z.B. vereinbart, dass Stillschweigen Zustimmung bedeuten soll.

34 Aus diesem Grund trägt die Anpassung der Begrifflichkeiten von «explicite» zu «exprès» im Vorentwurf nicht zur Klärung bei; die Verwendung des Begriffspaars «explizit» und «implizit» wäre weiterhin richtig, sofern der Bezug stimmt. Die EU übersetzt den Begriff der «ausdrücklichen Einwilligung» in der DSGVO im Übrigen mit «explicit consent» (vgl. z.B. Art. 9 abs. 2 Bst. a DSGVO).

35 Nicht entscheidend ist, ob auf dem Formular nur steht, dass die Daten für Marketingzwecke verwendet werden oder ob eine Einwilligungserklärung umfassender formuliert wird («Durch Abgeben des Formulars stimme ich zu, dass meine Daten für Marketingzwecke bearbeitet werden») oder das Formular gar unterschrieben wird. Letzteres wäre nur dann erforderlich, wenn die Einwilligung auch eine schriftliche sein müsste, was das DSG und der Vorentwurf jedoch nicht verlangt.

dar und wird auch in der Literatur zum Obligationenrecht als ausdrückliche Willenserklärung anerkannt.[36] Dies ist vor allem in einem Anwendungsfall der Praxis von zentraler Bedeutung: Der Anpassung von AGB. Diese wird normalerweise mit einer Klausel bewerkstelligt, wonach dem Kunden zugestellte Anpassungen von AGB als genehmigt gelten, wenn er ihnen nicht innert Frist widerspricht. Es handelt sich um eine klassische stillschweigende Zustimmung (*deemed consent*), die durchaus wirksam ist. Beschreiben die AGB, wie die Daten des Kunden bearbeitet werden, und widerspricht der Kunde nicht, so liegt diesbezüglich eine ausdrückliche Zustimmung im Sinne von Art. 4 Abs. 6 VE DSG vor. Das Schweigen als Zeichen der Zustimmung ist vereinbart und damit hinreichend, und die Zustimmung bezieht sich direkt auf den Inhalt der AGB und damit auch auf die darin explizit erwähnte Datenbearbeitung. Ob diese Datenbearbeitung so ungewöhnlich ist, dass darauf besonders hingewiesen werden muss, ist eine weitere Frage, die aber nichts mit jener der Ausdrücklichkeit zu tun hat. Die Frage der Ausdrücklichkeit hat auch nichts direkt mit der Frage der Information zu tun, die für eine informierte Einwilligung erforderlich ist, da diese Information sich auch auf die Konsequenzen der Einwilligung bezieht und daher ohne Weiteres breiter sein kann als der Bedeutungsgehalt des zustimmenden Verhaltens. Diese einzelnen Aspekte sind sauber zu trennen, und es bleibt zu hoffen, dass die Botschaft zum revidierten DSG diesbezüglich klarer ausfällt.

[Rz 35] Sinnvollerweise verzichtet wurde im VE DSG auf eine besondere Regelung zum Rückzug von Einwilligungen und zum *Bundling* von solchen, wie es in Art. 7 Abs. 4 DSGVO diskutiert wird; vor allem letztere Regelung ist auch im EU-Recht unklar und umstritten, da ein Bundling von Einwilligungen nach Art. 7 Abs. 4 DSGVO zwar verpönt, aber nicht *per se* unzulässig sein soll. Im Schweizer Recht können schon heute Einwilligungen in die Datenbearbeitung in der Regel zurückgezogen werden, wobei dies nur für die Zukunft gilt und entsprechende vertragliche Konsequenzen nach sich ziehen kann, wie etwa ein ausserordentliches Kündigungsrecht des betroffenen Unternehmens. Auch eine Regelung, wonach Datenschutzeinwilligungen in AGB oder sonst in Verträgen von anderen Einwilligungen getrennt erfolgen müssen, findet sich im VE DSG sinnvollerweise nicht. Es wäre auch nicht einzusehen, warum für den Datenschutz andere Standards gelten sollen als für andere Regelungsbereiche wie die Haftung, Gewährleistung oder Geheimhaltungspflichten.

## 5. Auslandtransfer: Komplizierter und langwieriger, aber nicht schwerer

[Rz 36] Die Regeln zur Bekanntgabe ins Ausland verändern sich grundsätzlich nicht. Es soll im revidierten DSG in materieller Hinsicht nicht schwieriger werden Daten ins Ausland zu übermitteln. Aber es wird aufgrund neuer Notifikations- und Genehmigungspflichten komplizierter, mitunter viel langwieriger und vor allem drohen neu empfindliche Sanktionen bei Verstössen.

[Rz 37] Die Eigenverantwortung im Rahmen der Bekanntgabe ins Ausland wird ein gutes Stück abgeschafft: War es bisher so, dass jeder Datenexporteur selbst beurteilen musste, ob seine Daten im Ausland noch angemessen geschützt sind, kann er sich neu auf den Entscheid des Bundesrates verlassen. Hat dieser festgestellt, dass das Recht im Zielstaat einen angemessenen Datenschutz

36 Ingeborg Schwenzer, Schweizerisches Obligationenrecht Allgemeiner Teil, Rn. 27.11; Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 8; Claire Huguenin, Obligationenrecht Allgemeiner und Besonderer Teil, Rn. 173; Wilhelm Schönenberger/Peter Jäggi, Zürcher Kommentar, Art. 1–17 OR, Art. 1, Rn. 145.

gewährleistet, so steht dem Art. 5 Abs. 1 VE DSG offenbar nichts mehr entgegen. Der Vorentwurf muss so zu verstehen sein, dass der Export selbst dann zulässig ist, wenn der Datenexporteur zum Schluss kommen sollte, dass er die Persönlichkeit der betroffenen Person schwerwiegend gefährdet, weil die Bekanntgabe die betroffene Person zum Beispiel einer Strafverfolgung im Ausland aussetzt.[37] Ist dies nicht die Absicht, dann wäre dieser Punkt zu klären. Ist diese Folge beabsichtigt, so kann und sollte Abs. 1 als überflüssig und verwirrend gestrichen und (etwa in Abs. 2) festgehalten werden, dass Personendaten *nur* dann exportiert werden dürfen, wenn einer der Fälle von Art. 5 und 6 VE DSG erfüllt ist (Angemessenheitsentscheid, Garantien, Ausnahmen). Wer einwendet, dass selbst bei Einhaltung der Fälle von Art. 5 und 6 VE DSG Situationen entstehen können, in welchen ein Export die Persönlichkeit einer betroffenen Person verletzt, so sei darauf hingewiesen, dass solche Konstellationen entweder über die Bearbeitungsgrundsätze in Art. 4 VE DSG oder aber über Art. 23 Abs. 1 VE DSG «gelöst» werden können, wenn auch ohne entsprechendes Sanktionsrisiko.

[Rz 38] Liegt kein Angemessenheitsbeschluss vor, kann weiterhin auf Basis von Standardklauseln, wie sie heute die Regel sind, exportiert werden. Eine Genehmigung ist nach wie vor nicht erforderlich; es gilt weiterhin nur eine Pflicht zur Information des EDÖB betr. den Einsatz solcher Verträge oder vergleichbaren Vorkehren (Art. 5 Abs. 6 VE DSG). In der Verordnung wird sich zeigen, ob hierzu neu weitere Angaben zu den konkreten Datentransfers nötig sind (wie sie der EDÖB heute ohne Rechtsgrundlage verlangt und einen unverhältnismässigen Aufwand mit sich bringen kann) oder weiterhin eine pauschale Information mit einem allgemeinen Hinweis auf die Verwendung der Standardklauseln ausreicht, was vollauf genügt. Welchen Sinn eine solche Informationspflicht hat und was sie zum Datenschutz beiträgt, ist allerdings schon unter dem heutigen Recht unklar; die Schweiz sollte die Informationspflicht streichen, wie schon die EU im Rahmen der DSGVO.

[Rz 39] Vom Standard abweichende Verträge («spezifische Garantien») können bei entsprechender Notifikation weiterhin benutzt werden (Art. 5 Abs. 3 Bst. b VE DSG). Binding Corporate Rules («BCRs») oder zu Deutsch «verbindliche unternehmensinterne Datenschutzvorschriften» benötigen hingegen neu eine Genehmigung durch den EDÖB (Art. 5 Abs. 3 Bst. d VE DSG). Dies ist inkonsequent, weil BCRs letztlich eine Untergruppe der «spezifischen Garantien» von Bst. b sind,[38] für welche lediglich eine Informationspflicht vorgesehen ist. Worin der Unterschied zwischen Garantien nach Bst. b und d besteht, bedarf daher einer Klärung, sollte an der Unterscheidung festgehalten werden; sie erscheint jedoch wenig sinnvoll. Offenbar gingen die Verfasser des Vorentwurfs davon aus, dass es Datenexportverträge für den «Einzelfall» gibt[39] und solche, die von Unternehmen (und Behörden) für mehrere verschiedene Datenübermittelungen eingesetzt werden, während nur letztere der Genehmigung bedürfen (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d VE DSG). Die meisten nicht standardisierten Verträge werden in letztere Kategorie fallen.

[Rz 40] Die Frist zur Genehmigung ist mit einem halben Jahr allerdings enorm lange angesetzt; bisher musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein. Das wird dazu

---

37 Die Erläuterungen VE DSG betonen jedenfalls für den Fall eines Angemessenheitsbeschlusses die Zulässigkeit des freien Datenverkehrs (S. 48).

38 Auch BCR werden regelmässig über (multilaterale) Verträge der einzelnen Gruppengesellschaften vereinbart. Sie kommen in der Regel dann zum Tragen, wenn nicht mit den Standardklauseln operiert werden soll (da in vielen EU-Ländern individuelle Verträge nur in Form von BCR möglich sind).

39 Erläuterungen VE DSG, S. 49, welche auf die Verwendung des Begriffs «im Einzelfall» Bezug nehmen, der sich jedoch nicht (mehr?) im VE DSG befindet.

führen, dass gerade nicht standardisierte Datenexportverträge in der Praxis völlig uninteressant werden, da kaum jemand ein halbes Jahr warten will, bevor er seinen Datentransfer durchführen kann. Hinzu kommt, dass die tatsächliche Frist sehr viel länger sein kann, da der EDÖB sich jederzeit auf den Standpunkt stellen kann, er habe noch nicht alle erforderlichen Informationen und die Frist von sechs Monaten somit von neuem zu laufen beginnt. Für BCRs ist immerhin vorgesehen, dass die Anerkennung durch eine andere Datenschutzbehörde auch für die Schweiz genügt, was insofern nicht sinnvoll ist, da BCR nur dann für die Schweiz genügen, wenn auch die Datentransfers *aus der Schweiz* erfasst sind. Dies wird bei der Prüfung durch eine ausländische Behörde nicht sichergestellt und muss in der Praxis erfahrungsgemäss immer wieder nachträglich angepasst werden, weil es vergessen ging.

[Rz 41] Als weitere Neuerung ist auch der Auftragsbearbeiter der Informations- bzw. Genehmigungspflicht unterworfen, nicht nur der Verantwortliche. Bisher hatte nur der Inhaber der Datensammlung eine Pflicht zur Notifikation. Die neue Regelung ist insbesondere in Konstellationen, in welchen der Verantwortliche in einem Land ohne angemessenen Datenschutz befindet, problematisch, so zum Beispiel Schweizer Cloud-Provider mit Kunden von ausserhalb Europas: Anerkannte Musterklauseln gibt es für diese Fälle nicht[40], und eigene Klauseln erfordern ein langwieriges Genehmigungsverfahren. Der Provider könnte sich zwar auf den Standpunkt stellen, dass vertragliche Garantien gar nicht erforderlich sind, weil mutmasslich die Einwilligung der betroffenen Personen für den Re-Export der Daten aus der Schweizer Cloud in das Land des Verantwortlichen vorliegt. Ob sich ein Provider angesichts der Strafsanktionen jedoch auf das Restrisiko einlassen wollen wird, ist eher fraglich. Diese Regelung sollte daher überdacht werden.[41]

[Rz 42] Die weiteren Rechtfertigungsgründe zur Übermittlung von Personendaten in Länder ohne angemessenen Datenschutz finden sich neu in einem separaten Artikel (Art. 6 VE DSG). Als wichtige Anpassung ist hier der Fall zu nennen, dass Unterlagen zwecks Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ins Ausland übermittelt werden. Solche Transfers waren in ein Land ohne angemessenen Datenschutz wie etwa die USA bisher nur möglich im Zusammenhang mit Gerichtsverfahren, nicht jedoch Untersuchungen durch andere Behörden. Letztere sind neu ebenfalls abgedeckt; gestützt auf dem Sinn und Zweck der Erweiterung sollte der verwendete Begriff der «Verwaltungsbehörde» nicht nur Aufsichtsbehörden erfassen, sondern alle Behörden, vor welchen Verfahren zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen stattfinden können, also etwa eine Kartellbehörde, eine Steuerbehörde oder auch eine Behörde, die strafrechtliche Tatbestände untersucht und allenfalls sogar vergleichsweise regelt, wie dies etwa die *Criminal Division des US Departement of Justice* regelmässig tut. Unter heutigem Recht fallen diese Fälle zwischen Stuhl und Bank, was in weit über hundert Datenschutzprozessen vor Schweizer Gerichten im Zusammenhang mit dem US-Steuerstreit zur Blockierung von Datenlieferungen in die USA führte.[42] Diese Fälle waren denn auch der Anlass für die Erweiterung. Um Verwirrungen über die Frage zu vermeiden, was genau mit «Verwaltungsbehörden» gemeint ist,

40 Die *Controller-Processor-Clauses* der EU funktionieren nur in die umgekehrte Richtung.

41 Immerhin ist zu erwähnen, dass es im Falle von «*Processor-BCRs*» durchaus Konstellationen gibt, in welchen der Auftragsbearbeiter in die Pflicht genommen werden muss. Im heutigen Recht wird so verfahren, dass solche Regelungen durch Auftragsbearbeiter dem EDÖB zur Vorprüfung vorgelegt werden, dieser dann aber im konkreten Einzelfall jeweils nochmals prüft, ob sie hinreichend sind.

42 Vgl. etwa David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 594 ff.

empfiehlt es sich wie in der DSGVO[43] den Zusatz «vor einem Gericht oder einer Verwaltungsbehörde» zu streichen. Hierbei kann ferner die Wendung, dass die Bekanntgabe «unerlässlich» sein muss, an den Wortlaut der DSGVO angeglichen werden, die von «erforderlich» spricht. Zwar verwendet schon das bisherige Recht das Wort «unerlässlich». Es wird jedoch nicht wortwörtlich verstanden: Alles, was in einem entsprechenden Verfahren an Unterlagen Eingang finden soll oder von der Gegenpartei verlangt werden kann, ist damit erfasst.[44] Ebenso ist nicht nur die aktive Durchsetzung von Ansprüchen erfasst, sondern ebenso die Abwehr und Verteidigung gegen Rechtsansprüche. Damit der neue Wortlaut der Bestimmung überhaupt Sinn macht, ist der Begriff der «Rechtsansprüche» so zu verstehen, dass er auch straf- oder verwaltungsrechtliche Massnahmen umfasst. Dies wäre mindestens in der Botschaft klarzustellen.

[Rz 43] Gegenüber heutigem Recht nicht geändert, wurde die Ausnahmeregelung für Bekanntgaben im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags mit der betroffenen Person. Damit ist die Schweiz allerdings strenger als die DSGVO. Letztere erlaubt die Bekanntgabe auch dann, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist.[45] Diese Ergänzung wäre auch für das Schweizer Recht sinnvoll. Sie sollte aus Gründen der Konsistenz auch im Rahmen von Art. 24 Abs. 2 Bst. a VE DSG vorgenommen werden.

[Rz 44] Eine besonders heikle neue Bestimmung findet sich schliesslich in Art. 6 Abs. 2 VE DSG: Sie verlangt, dass Datenexporte in etlichen Konstellationen dem EDÖB gemeldet werden müssen, so auch in allen Fällen, in welchen der Export durch Vertragsabschluss oder -erfüllung oder ein ausländisches Rechtsverfahren gerechtfertigt wird. Dies wird nicht nur zu zahlreichen Meldungen führen, die der EDÖB gar nicht vernünftig oder innert nützlicher Frist bearbeiten können wird. Sie zwingt Unternehmen faktisch auch, dem EDÖB sensible Geschäftsgeheimnisse wie etwa laufende ausländische Untersuchungen und Gerichtsverfahren offenzulegen, wofür es keinen guten Grund gibt. Hierbei ist zu beachten, dass alle dem EDÖB gelieferten Unterlagen gemäss Öffentlichkeitsgesetz öffentlich einsehbar sind, einschliesslich Meldungen nach Art. 6 VE DSG. Geschäftsgeheimnisse sind zwar nach dem Buchstaben des Gesetzes vom EDÖB zu schützen, doch hat er diesen Schutz bisher sehr eng ausgelegt. Geschwärzt wird in der Praxis nur sehr wenig. Zur Meldung ist zudem nicht nur der Verantwortliche verpflichtet, sondern auch der Auftragsbearbeiter, obwohl er regelmässig nicht über die erforderlichen Angaben verfügen wird und nicht Herr der Daten ist. Es ist zu hoffen, dass diese Meldepflicht ersatzlos gestrichen wird.

## 6. Deutlich erweiterte Informations- und Auskunftspflichten

[Rz 45] Die Informationspflicht in Art. 13 VE DSG wird in der Praxis eine der materiell wichtigsten Neuerungen des revidierten DSG für private Datenbearbeiter sein. Sie sieht eine Informationspflicht im Rahmen jeder Datenbeschaffung vor, die deutlich weitergeht als das, was bisher erforderlich war. Sie ist wie der bisherige Art. 14 DSG kein Bearbeitungsgrundsatz, sondern eine öffentlich-rechtliche Norm, deren Verletzung nicht zwingend eine Persönlichkeitsverletzung zur Folge hat, dafür strafrechtlich sanktioniert wird. Anders als bisher erfasst die neue Infor-

43 Vgl. Art. 49 Abs. 1 Bst. e DSGVO.

44 David Rosenthal, Handkommentar DSG, Art. 6, N 66.

45 Art. 49 Abs. 1 Bst. c DSGVO.

mationspflicht jede Datenbeschaffung, d.h. es muss immer informiert werden. Der Katalog der Ausnahmen ist wesentlich enger als bei der generellen Transparenzpflicht nach Art. 4 VE DSG.

[Rz 46] Die Bestimmung ist in verschiedener Hinsicht problematisch. Zunächst ist unklar, über welche Dinge informiert werden muss. Art. 13 Abs. 2–4 VE DSG zählen zwar einige konkrete Angaben auf, doch muss die Information alles umfassen, was für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen. Gemäss den Erläuterungen soll die Beschränkung auf Mindestangaben eine flexible Handhabung der Informationspflicht erlauben und so zu viele Informationen verhindern. Da die Informationspflicht aber strafrechtlich massiv sanktioniert ist und sogar die fahrlässige Verletzung strafbar sein soll, werden Verantwortliche und Auftragsbearbeiter zur Risikominimierung wesentlich mehr Informationen liefern, als sie müssen, da sie sich auf ihre eigene Beurteilung, was an Informationen wirklich sinnvoll ist, nicht verlassen werden wollen.

[Rz 47] Es ist daher davon auszugehen, dass viele Schweizer Unternehmen sich an die umfassenderen Vorgaben der DSGVO halten werden.[46] In einem Punkt geht der VE DSG allerdings über die DSGVO hinaus: Nach Art. 13 Abs. 4 VE DSG muss auch über die Identität und Kontaktdaten der Auftragsbearbeiter informiert werden. Dies geht nach der hier vertretenen Auffassung viel zu weit und bringt betroffenen Personen in der Regel keinen Mehrwert. Hier sollte die Regelung darauf beschränkt werden, dass diese Information wenn überhaupt nur im Rahmen des Auskunftsrechts auf spezifische Nachfrage geliefert werden muss.[47] Über die DSGVO hinaus geht auch Art. 13 Abs. 5 VE DSG, der eine Information der betroffenen Person bei indirekter Datenbeschaffung spätestens bei Speicherung vorsieht; die DSGVO gewährt hier eine Frist von bis zu einem Monat.[48]

[Rz 48] Unklar im Rahmen der Bestimmung bleibt ferner, ob dann, wenn nachträglich neue Bearbeitungszwecke hinzukommen, «nachinformiert» werden muss; das dürfte (weiterhin) wohl nicht der Fall sein. Das gilt auch für die anderen Punkte, über die informiert werden muss. Es wird daher nur darüber informiert werden müssen, was schon zum Zeitpunkt der Beschaffung feststand; liegt eine laufende Beschaffung vor, genügt es, die Information für die künftig erfolgenden Beschaffungen anzupassen. Sollen bestehende Daten zu einem neuen Zweck bearbeitet werden, wird hierfür eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich werden, soweit es kein mit dem ursprünglichen Zweck vereinbarer Zweck darstellt (dazu Rz 24 oben). Der Schutz der betroffenen Person wird so z.B. auch bei der Erweiterung der Kategorien der Empfänger sichergestellt. Etwas anderes wäre in letzter Konsequenz auch absurd, wenn pauschal nachinformiert werden müsste, wenn sich die Umstände, über die informiert wurde, geändert haben: Man stelle sich vor, ein Unternehmen ändert seine Kontaktadresse und müsste deswegen alle Personen, von denen es je Daten beschafft hat, darüber in Kenntnis setzen. Natürlich könnte argumentiert werden, dass dies nötig sei, damit diese Personen weiterhin wissen, wo sie ihre Rechte geltend machen können, aber eine solche Regelung würde jedes vernünftige Mass missen.

[Rz 49] Ohnehin ist absehbar, dass die Informationspflicht zu einer unnötigen, ja sogar kontraproduktiven Überinformation der betroffenen Personen führen wird, die kaum einen wirksamen Beitrag zur Verbesserung des Datenschutzes leisten wird. Die DSGVO geht punkto Informations-

46 Vgl. Art. 13 und 14 DSGVO.

47 Art. 20 VE DSG sieht die Information ebenfalls vor.

48 Art. 14 Abs. 3 Bst. a DSGVO.

pflicht zwar bezüglich der Elemente, über die informiert werden muss, noch weiter, doch wird dort inzwischen ebenfalls deutliche Kritik laut. Eine risikobasierte Transparenzpflicht, wie sie in Art. 4 DSG und VE DSG enthalten ist, genügt völlig.

[Rz 50] Eine im Vorfeld vorgeschlagene Lösung, wonach es genügen soll, dass ein Unternehmen statt einer Detailinformation bei jeder Datenbeschaffung mit einer Information auf seiner Website arbeiten kann, fehlt leider im Vorentwurf. Sie ermöglicht einen einigermassen sinnvollen Umgang mit der Informationsflut für jene, die diese Informationen tatsächlich erhalten möchten. Diese wenigen betroffenen Personen könnten sich dann auf den Webseiten der betreffenden Unternehmen im Detail darüber ins Bild setzen, wofür diese ihre Daten verwenden. Die Information am Beschaffungspunkt könnte auf die Identität und Information für weitergehende Informationen beschränkt werden; da der Zugang zu dieser Information gesichert wäre, wären auch die Vorgaben der Konvention 108 erfüllt. Die Lösung entspricht auch der heutigen Praxis des EDÖB. Es soll jedoch gemäss den Erläuterungen zum Vorentwurf gerade nicht genügen, wenn die betroffene Person nach der Information suchen oder fragen muss.[49] Dies dürfte bedeuten, das inskünftig überall, wo im Alltag Personendaten beschafft werden mit entsprechend langen (und entsprechend kleingedruckten) Informationstexten gerechnet werden muss, damit die Vorgaben von Art. 13 VE DSG der guten Form halber erfüllt sind. Wird die Norm ernst genommen, wird beispielsweise neben Sicherheitskameras in einem Gebäude jeweils ein Schild mit einem entsprechenden Informationstext befestigt werden müssen. Bisher genügte es, dass die Kameras sichtbar waren; alles andere ergab sich aus dem Zusammenhang, und wer mehr wissen wollte, konnte nachfragen und Auskunft erhalten.

[Rz 51] Der Katalog der Ausnahmen in Art. 14 VE DSG entspricht in Teilen der bisherigen Ausnahmeregelung von Art. 9 DSG, ist jedoch nach der hier vertretenen Auffassung zu eng und enger, als sie es gemäss der revidierten Konvention 108 sein müsste. So ist die Berufung auf überwiegende private Interessen nur dann möglich, wenn die Personendaten nicht an Dritte weitergegeben werden (Art. 14 Abs. 4 Bst. a VE DSG). Es ist dies eine schon im bisherigen Recht vorgesehene Einschränkung, für die es keine Berechtigung gibt. Entscheidend kann letztlich nur sein, ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person überwiegt. Tut es das im konkreten Fall, ist damit bereits gesagt, dass eine Information nicht mehr sinnvoll und auch nicht legitim ist. So werden sich Konzerne, die ihre Daten konzernintern nicht nur für die Zwecke der Auftragsbearbeitung teilen, bei der heutigen Regel nie auf überwiegendes eigenes Interesse berufen können, während es Unternehmen, die aus nur einer einzigen juristischen Person bestehen, können. Auch die Weitergabe an Behörden – zum Beispiel eine Aufsichtsbehörde – führt dazu, dass ein Unternehmen sich nicht mehr auf die Ausnahmebestimmung berufen kann, selbst wenn es ansonsten gute Gründe dafür gäbe. Es ist zu hoffen, dass der betreffende Zusatz gestrichen wird.[50]

[Rz 52] Es sollte zudem erwogen werden, die typischen Ausnahmefälle im Gesetz analog dem heutigen Art. 13 Abs. 2 DSG (bzw. Art. 24 VE DSG) klarzustellen, wobei dies für das Auskunftsrecht nach Art. 20 VE DSG (dazu sogleich) wichtiger ist als für die Pflicht zur Information nach Art. 13 VE DSG. So besteht zum Beispiel heute und unter dem Vorentwurf kein pauschales Recht, die Herausgabe der Kommunikation zwischen Unternehmen und Anwalt zu verweigern. Wäh-

49 Erläuterungen VE DSG, S. 56.

50 Gemeint ist: «und er die Personendaten nicht Dritten bekannt gibt».

rend ein Unternehmen dies in einem zivilrechtlich, strafrechtlichen und verwaltungsrechtlichen Verfahren ohne Weiteres kann, ist dies beim Auskunftsrecht nicht der Fall. Hier muss, soweit überhaupt zulässig, mit überwiegenden eigenen Interessen im Einzelfall argumentiert werden. Das erscheint stossend. Als weitere überwiegende private Interessen fallen gemäss heute herrschender Lehre und Praxis insbesondere in Betracht Daten zur internen Meinungsbildung[51], Sicherheitsinteressen (z.B. keine Mitteilung der Aufbewahrungsdauer von Daten zur Bekämpfung von Missbräuchen), die Lieferung von Unterlagen, die der Auskunftspflichtige schon hat (z.B. nutzen Bankkunden das Auskunftsrecht heute, um kostenlos Kontoauszüge nachzubestellen, die sie verloren haben, da Datenschutzgründe immer vorgeschoben werden können), zum Schutz von eigenen Geheimhaltungsinteressen (heute führt das Auskunftsrecht mitunter zur absurden Situation, dass einem Mitarbeiter zwar verboten werden kann, Geschäftsunterlagen mit nach Hause zu nehmen oder privat zu nutzen, sie ihm aber kostenlos in Kopie zur privaten Nutzung übergeben werden müssen, wenn er darin erwähnt wird und er sie unter Vorwand des Datenschutzes nach Art. 8 DSG herausverlangt, selbst wenn er das Unternehmen längst verlassen hat).

[Rz 53] Dass die Informationspflicht nach Art. 14 Abs. 2 Bst. b VE DSG auch entfällt, wenn die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist, ist bezüglich der Berufung auf überwiegende eigene Interessen keine Lösung: Die Ausnahme gilt nur, wenn die Informationen nicht bei der betroffenen Person direkt beschafft werden, und sie soll gemäss den Erläuterungen eng ausgelegt werden.[52] Werden beispielsweise für ein Gerichtsverfahren Beweismittel zusammengetragen, so wird künftig bei wortgetreuer Auslegung der Norm versucht werden müssen, alle darin erwähnten Personen[53] zu kontaktieren, um sie darüber zu informieren, dass die Unterlagen möglicherweise im Prozess eingereicht werden, auch wenn das Verfahren sie aller Voraussicht nach nicht tangiert. Eine Berufung auf überwiegende private Interessen ist aufgrund der Weitergabe an Dritte nicht möglich. Findige Köpfe werden argumentieren, es liege ein Fall von Art. 14 Abs. 2 Bst. a VE DSG vor, nämlich dass die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist, doch das gilt, wenn überhaupt, nur für Verfahren vor Schweizer Gerichten und zweitens nur für Dokumente, die als Beweismittel auch eingereicht werden. Auch Art. 14 Abs. 3 Bst. a VE DSG greift nicht, da diese Bestimmung nur dann den Verzicht auf die Information erlaubt, wenn ein Gesetz die Preisgabe der Information verbietet, wie z.B. der Bank mit Bezug auf vom Bankgeheimnis geschützte Daten. Schreibt das Gesetz die Bearbeitung von Daten lediglich vor, muss informiert werden; die Ausnahme von Art. 14 Abs. 2 Bst. a VE DSG greift nur, wenn die Daten über Dritte beschafft werden. Eine Bank müsste also genau genommen im Börsenhandel inskünftig jeden Händler, mit welchem sie zu tun hat, darüber informieren, dass die Telefonate aufgezeichnet und Daten über ihn aufbewahrt werden (mit allen Angaben gemäss Art. 13 VE DSG), weil die FINMA dies so verlangt, wobei sie dies nicht einmal in Form einer gesetzlichen Regelung, sondern im Rahmen ihrer «Rundschreiben» tut. Der Ausnahmekatalog von Art. 14 VE DSG sollte somit auch diesbezüglich erweitert werden, etwa indem in Abs. 1 auch jene Fälle erfasst werden, in denen sich die Datenbearbeitung aus Gesetz ergibt, in den betroffenen Verkehrskreisen als bekannt gilt oder sich aus den Umständen ergibt.

---

51 Vgl. Entscheid Bezirksgericht Zürich vom 2. Februar 2015, zitiert in: David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 600.

52 Erläuterung VE DSG, S. 58.

53 Z.B. Mitarbeiter anderer Unternehmen, die E-Mails gesandt, Verträge unterzeichnet haben oder sonst erwähnt sind.

Dies kann allenfalls durch eine Pflicht abgefedert werden, die Detailinformationen online oder auf Nachfrage bereitzustellen.

[Rz 54] Die Ausnahmen von Art. 14 VE DSG werden auch für das Auskunftsrecht von Relevanz sein, welches neu in Art. 20 VE DSG geregelt ist und bezüglich seiner Ausnahmen ebenfalls auf Art. 14 VE DSG verweist. Hier war erwartet – oder erhofft – worden, dass der Vorentwurf Massnahmen vorsieht, um dem grassierenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke Einhalt zu gebieten, was jedoch nicht geschah.[54]

[Rz 55] Stattdessen soll das Auskunftsrecht ausgebaut werden. Insbesondere sind weitere Informationen hinzugekommen, über die informiert werden muss, wie zum Beispiel die Aufbewahrungsdauer oder Kriterien zu ihrer Festlegung und die Identität und Kontaktdaten aller Auftragsbearbeiter. Weggefallen sind Angaben zu den Rechtsgrundlagen der Bearbeitung. Unter diesen Titel hatte das Zürcher Obergericht sogar die Herausgabe von Unterlagen angeordnet, welche keinerlei Personendaten der betroffenen Person enthielt – ein Fehlurteil.[55]

[Rz 56] In Art. 14 VE DSG fehlt auch ein Vorbehalt zugunsten von Datenbearbeitungen, welche gesetzlich vorgesehen sind.

[Rz 57] Gestrichen wurde immerhin die bisherige Regelung, wonach die Auskunft in der Regel schriftlich ist, in Form eines Ausdrucks oder einer Fotokopie zu erteilen ist. Sie muss aber kostenlos sein. Interessanterweise fehlt eine Norm, welche den Bundesrat ermächtigt, diese Punkte auf Verordnungsebene zu regeln, so namentlich Ausnahmen von der Kostenlosigkeit vorzusehen, wie dies die DSGVO tut.[56] Auch diese Aspekte des Auskunftsrechts hat in der Vergangenheit immer wieder zu Rechtsstreitigkeiten geführt, da das Auskunftsrecht von ehemaligen Mitarbeitern benutzt wurde, um für ihre Zwecke an Kopien ihrer eigenen Geschäftskorrespondenz und weiterer Geschäftsunterlagen, an denen sie beteiligt waren, zu gelangen. Da dem Bundesrat keine Kompetenz zur Definition von Ausnahmen von der Kostenlosigkeit eingeräumt werden soll, wird es nicht möglich sein, solche Fälle auf dem Verordnungsweg vorzusehen. Die Auskunft muss selbst bei querulatorischen, wiederholten und extrem aufwändigen Anfragen gratis sein, was stossend erscheint. Ein Auskunftsersuchen kann, wenn es eine etwas speziellere Materie betrifft, ohne Weiteres viele Tausend Franken kosten. Selbst beim Öffentlichkeitsgesetz (BGÖ) darf der Staat für seine Umtriebe Kostenersatz verlangen.

---

54 Lösungsansätze gibt es diverse. Sie reichen von der Beschränkung auf Fälle, in denen nachgewiesen werden kann, dass ein Auskunftsersuchen primär aus Datenschutzgründen erfolgt und nicht zum Zwecke der Beweisausforschung (Frage des Institutsmissbrauchs) über Kostenschranken bis hin zu einer Klarstellung, dass die Hürden zur Annahme eines Missbrauchs deutlich zu senken sind. Einer der erfolgversprechendsten Ansätze erscheint jedoch, das Auskunftsrecht inhaltlich nicht einzuschränken, es aber formal so auszugestalten, dass es für die Beweisausforschung nicht mehr interessant ist. Dies könnte zum Beispiel dadurch geschehen, dass der Auskunftspflichtige wählen kann, dass er die Daten nicht mehr in Kopie dem Auskunftsersuchenden übergibt, sondern stattdessen einer dritten Stelle, die entweder die Verletzung des Datenschutzes stellvertretend prüft (denn nur dazu dient das Auskunftsrecht), wie es der EDÖB heute in gewissen Fällen tut, oder bei welcher der Auskunftsersuchende die Daten einsehen kann, aber sie eben nicht mehr zweckentfremdet verwenden kann, z.B. als Beweismittel in einem nicht datenschutzrechtlich motivierten Forderungsprozess, was heute den Regelfall darstellt.

55 OGer vom 5. Dezember 2014 (LB140073-O3-1), E. 7; dazu David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 591 ff.

56 Art. 12 Abs. 5 Bst. a DSGVO.

## 7. Profiling und Einzelfallentscheide

[Rz 58] Auf den neuen Begriff des Profiling wurde bereits eingegangen. Demnach soll ein Profiling ohne ausdrückliche Einwilligung der betroffenen Person neu *per se* eine Persönlichkeitsverletzung darstellen. Dies ist gegenüber dem heutigen Recht eine deutliche Verschärfung, da bisher nur die *Weitergabe* von Persönlichkeitsprofilen eine Rechtfertigung erforderte. Die DSGVO kennt keine solche Regelung. Da dort jedoch jede Datenbearbeitung eine Rechtfertigung erfordert und im Falle besonders schützenswerter Personendaten eine ausdrückliche und eine solche auch im Falle eines automatisierten Profiling erforderlich ist, welches rechtliche oder in ähnlich erheblicher Weise auf eine Person wirkt, fällt die Regelung der DSGVO im Ergebnis nur etwas milder aus als die Schweizer Regelung.

[Rz 59] Neu findet sich im Vorentwurf auch eine Regelung zu automatisierten Einzelfallentscheiden. Eine solche Regelung war schon im Rahmen der letzten Revision des DSG diskutiert, dann aber wieder verworfen worden. In der EU sind solche schon heute eingeschränkt. Nun verlangt sie die revidierte Konvention 108. Im Kern geht es darum, dass bei automatisierten Einzelentscheiden, welche rechtliche oder erhebliche Auswirkungen auf eine Person haben, dieser Person ein Recht auf Anhörung durch einen Menschen gewährt wird. Dieser Anspruch auf «menschliches Gehör» findet sich neu in Art. 15 VE DSG. Die Anhörung kann vor oder nach dem Einzelentscheid stattfinden, und in dessen Rahmen verlangt das Schweizer Recht auch, dass die Person sich zu den über sie bearbeiteten Personendaten äussern können muss. Dies wiederum setzt sachlogisch eine Information über solche Entscheide voraus, die ebenfalls in Art. 15 VE DSG statuiert wird; unklar bleibt, wie allgemein die Information sein kann, was aber einen erheblichen Unterschied ausmachen kann.[57] Weiter stellt sich die Frage, ob nicht nur über die Tatsache eines automatisierten Entscheids informiert werden muss, sondern auch über die dazu bearbeiteten Personendaten, da sich die Person dazu ebenfalls äussern können muss; hier sollte darauf hingewiesen werden, dass diese Angaben nur auf Rückfrage zu liefern sind. Alles andere wäre uferlos. Da eine Person aber unabhängig von Art. 15 VE DSG die Möglichkeit hat, sich zu den über sie bearbeiteten Personendaten zu äussern, namentlich auch im Rahmen von Art. 4 Abs. 5 VE DSG, kann dieses Recht aus Art. 15 Abs. 2 VE DSG ohne Verlust gestrichen werden; die DSGVO sieht ein Recht zur Äusserung zu den bearbeiteten Daten in der Regelung zu automatisierten Einzelentscheiden auch nicht vor.[58]

[Rz 60] Aus dem Zusammenhang ergibt sich auch, dass der Entscheid zum Zeitpunkt der Anhörung nicht definitiv sein darf, auch wenn er von der «Maschine» schon gefällt worden ist. Es genügt also im Prinzip, bei automatisierten Einzelentscheiden eine Telefonnummer oder sonstige Kontaktmöglichkeit anzugeben, wo sich eine betroffene Person hinwenden kann, wenn sie sich zum Entscheid äussern möchte. Die Äusserung muss von einer Person zur Kenntnis genommen werden, welche bewirken kann, dass das Unternehmen auf seinen Entscheid zurückkommt; einfach nur entgegennehmen und ablegen wird nicht genügen (ähnliche Regelungen gibt es heute schon in anderen Bereichen, so z.B. Art. 333a Abs. 2 OR).

---

57 Eine allgemeine Klausel, wonach das Unternehmen auch automatisierte Einzelentscheide durchführt, wird allerdings nicht genügen. Es wird mindestens verlangt werden können, dass genügend Angaben geliefert werden, um automatisierte Entscheide als solche erkennen zu können. Die Schwierigkeit besteht allerdings nicht in den ohnehin der betroffenen Person kommunizierten Entscheiden, sondern jenen, die sowieso nicht kommuniziert werden (vgl. das nachfolgend erwähnte Schulbeispiel eines Viren- und E-Mail-Scanners, der jede Mail automatisiert daraufhin prüft, ob sie zugestellt wird; eine Mitteilung an den Absender erfolgt bestenfalls bei Nichtzustellung).

58 Art. 22 DSGVO.

[Rz 61] Anwendungsfälle sind gemäss Erläuterungen Situationen, in welchen ein Computer alleine darüber entscheidet, ob und zu welchen Konditionen ein Vertrag abgeschlossen wird oder Verkehrsbussen, die aufgrund einer Bildaufnahme automatisch verschickt werden.[59] Aber der Anwendungsbereich ist sehr viel breiter und umfasst etwa auch automatisierte Sicherheitskontrollen in Computernetzwerken wie z.B. im Falle von Spam- und Virenscannern, die E-Mails blockieren oder von den anderen separieren, Systeme zur Betrugsbekämpfung, welche z.B. Kreditkarten bei verdächtigen Transaktionen automatisch sperren und letztlich jeden etwas professionelleren Online-Shop, der automatisch Verträge abschliesst. In all diesen Fällen wird neu nicht nur über die Einzelentscheide informiert, sondern auch eine Möglichkeit zum Dialog mit einem Menschen vorgesehen werden müssen. Ausnahmen sieht Art. 15 VE DSG keine vor, die DSGVO hingegen lässt solche zu.[60] Weitere Beispiele sind Glücksspielsysteme, in welchem der Computer (sprich: Der Zufallsgenerator) über den Gewinn des Spielers entscheidet, selbstfahrende Autos oder automatische Börsenhandelssysteme. Sie sind zwar nur dann erfasst, wenn sie Personendaten bearbeiten, doch dies ist in allen drei Fällen ohne Weiteres denkbar.[61] Unklar wiederum ist, inwiefern auch automatisierte Abwicklungssysteme, wie etwa im Internet-Banking, erfasst sind. Ziel der Regelung sind sie sicher nicht, aber aufgrund der weitgefassten Definition und der Tatsache, dass heutzutage schon aus Gründen der Effizienz sehr viele Routineentscheide dem Computer übertragen werden, besteht das Risiko, dass sehr viele Fälle erfasst sind. Besonders hart wird dies die Bundesorgane treffen, da sie hierfür neu eine formelle Gesetzesgrundlage haben müssen (Art. 27 Abs. 2 VE DSG): Ohne eine Gesetzesanpassung wird ein Bundesorgan unter dem neuen DSG somit Computer selbst im Massengeschäft nicht mehr ohne Weiteres zur Effizienzsteigerung einsetzen können[62], was sicherlich nicht im Sinne des Erfinders wäre. Der Vorentwurf sieht solche Anpassungen nicht vor; viele der Anpassungen in anderen Gesetzen beschränken sich auf die Streichung der Erwähnung der Persönlichkeitsprofile.

[Rz 62] Die Erläuterungen zum Vorentwurf sprechen zwar davon, dass die Auswirkungen einer automatisierten Einzelentscheidung einen gewissen Schweregrad erreichen müssen, um erfasst zu sein.[63] Eine beliebige rechtliche Wirkung soll jedoch genügen. Wird in einer Online-Auktion automatisch darüber entschieden, wer den Zuschlag erhält, liegt eine rechtliche Wirkung vor und der Plattformbetreiber wird allen Mitbietern in diesem Fall die Möglichkeit geben müssen, sich zu äussern, auch wenn dies in der Sache völlig unsinnig ist. Noch absurder ist das Beispiel mit den Glückspielen: Sie müssten künftig konsequenterweise datenschutzrechtlich verboten werden, da sie immer rechtliche Wirkungen haben (der Computer entscheidet über die Pflicht zur Auszahlung von Gewinn), ausser der Spieler bleibt anonym oder es wird ihm die Möglichkeit gegeben, mit dem Betreiber darüber zu sprechen, warum er nicht gewonnen hat und warum das falsch ist.

---

59 Erläuterungen VE DSG, S. 59.

60 Art. 22 Abs. 2 Bst. b DSGVO.

61 Man denke an Online-Glückspiele oder Glückspiele, für welche sich eine Person anmelden muss, an selbstfahrende Autos, die über ihre Kameras Bilder von anderen Verkehrsteilnehmern machen, oder Handelssysteme, die es mit einem menschlichen Börsenteilnehmer als Gegenseite zu tun haben.

62 Ein Beispiel sind z.B. die heute bei Krankenkassen im obligatorischen Bereich eingeführten Systeme zur automatisierten Abrechnung.

63 Automatisierte Einzelfallentscheide gibt es überall im Alltag. Auch eine automatische, Badge-basierte Liftsteuerung kann z.B. eine solche sein. So entscheidet im Bürogebäude des Autors dieses Beitrags ein Computer alleine darüber, ob einem Mitarbeiter eine Liftkabine mit einer eingebauten Videokamera oder eine Liftkabine ohne zugeteilt wird, d.h. ob mehr oder weniger gewichtig in die Privatsphäre des Mitarbeiters eingegriffen wird.

[Rz 63] Fristen hierfür für die Anhörung der betroffenen Person sieht Art. 15 VE DSG allerdings keine vor, auch keine spezifische Form. Immerhin muss die Anhörung kostenlos sein.[64] Zu erwähnen ist, dass die Konvention 108 eine derart strenge Regelung nicht verlangt; auch hier geht die Schweiz weiter als nötig.

[Rz 64] Anders als in der DSGVO schaltet der Vorentwurf das Profiling den automatisierten Einzelentscheiden nicht gleich. In der DSGVO ist jedes automatisierte Profiling ein automatisierter Einzelentscheid und als solcher bei hinreichender Auswirkung geregelt; sonst gelten für das Profiling keine besonderen Bestimmungen. In der Schweiz schlägt der Vorentwurf eine breitere Regelung vor, indem auch «menschliches» bzw. manuelles und nicht nur ein maschinelles Profiling erfasst werden soll und daher eine Regelung unabhängig von automatisierten Einzelentscheiden erforderlich wurde. Ob das wirklich sinnvoll ist, ist eine andere Frage.

[Rz 65] Der Vorentwurf geht allerdings auch im Falle der automatisierten Einzelentscheide noch viel weiter als die DSGVO, indem in den Auskunftspflichten ein Verantwortlicher verpflichtet wird, bei *jedem* Entscheid, den er trifft und welchem die Bearbeitung von Personendaten zugrunde liegt, einer betroffenen Person Rechenschaft darüber abzulegen, wie und warum er so entschieden hat und welche Konsequenzen dies für die betroffene Person zusätzlich zu den Daten hat, die er hierzu verwendet hat. Diese Regel in Art. 20 Abs. 3 VE DSG gilt zwar insbesondere für automatisierte Einzelentscheide, aber ausdrücklich nicht nur. Eine solch breite Auskunftspflicht ist völlig überzogen und greift massiv in die Freiheiten der Unternehmen und betroffenen Privatpersonen ein. Stellt eine Person einer Firma eine Werbung für ein Angebot zu und entscheidet sich die Firma, diese Werbung in den Abfall zu werfen, so soll sie der Person für diesen Entscheid auf Nachfrage gemäss Vorentwurf rechenschaftspflichtig bleiben. Doch selbst wenn die Regel auf automatisierte Einzelentscheide beschränkt würde, wäre sie unsinnig: Diesfalls bliebe die Firma für ihren Viren- und Spamfilter rechenschaftspflichtig, um ein Beispiel zu nennen. Sinn macht eine Auskunftspflicht höchstens im Zusammenhang mit automatisierten Einzelentscheiden, die auch Anspruch auf «menschliches Gehör» gewähren, also gewisse Auswirkungen haben. So sieht es auch die DSGVO vor.[65]

[Rz 66] Es sollte zudem klargestellt werden, dass selbst in diesen Fällen nur dann Auskunft zu erteilen ist, wenn spezifisch nach den Zusatzdaten zu einem bestimmten Entscheid gefragt wird. Was nicht zugelassen werden sollte, wäre ein Ersuchen im Sinne von «gebt mir eine Liste aller automatisierten Einzelentscheide, die Ihr in Eurem Unternehmen trefft». Dies würde massiv in die Privatsphäre der Unternehmen eingreifen und dient primär der Ausforschung oder Schikane. Da die betroffene Person im Falle eines automatisierten Einzelentscheids ohnehin konkret auf diesen hingewiesen werden muss, genügt es, die Auskünfte nach Art. 20 Abs. 3 VE DSG auch nur in den Fällen zu gestatten, wo die betroffene Person diesem automatisierten Einzelentscheid unterworfen ist. Da sie ein Anhörungsrecht hat, genügt es, wenn sie die Auskunft vor ihrer konkreten Stellungnahme zum Entscheid erhält; eine Anfrage «auf Vorrat» ist somit nicht nötig.

64 Erläuterungen VE DSG, S. 60.

65 Art. 15 Abs. 1 Bst. h DSGVO.

## 8. Recht auf Vergessen, Widerspruchsrecht, Weitermeldepflicht

[Rz 67] Trotz erheblicher öffentlicher Diskussionen im Vorfeld der Vorlage[66] soll sich gemäss Vorentwurf am «Recht auf Vergessen» nichts ändern. Das ist völlig richtig so, denn das Schweizer Recht kennt schon heute eine umfassende und ausgewogene Regelung, die einer betroffenen Person erlaubt, sich gegen eine Datenbearbeitung in welcher Weise auch immer auszusprechen. Sie war bisher in Art. 12 DSG enthalten und findet sich nun unverändert in Art. 23 Abs. 2 Bst. b VE DSG.

[Rz 68] Der zivilrechtliche Rechtsschutz ist neu in Art. 25 VE DSG geregelt und entspricht ebenfalls dem heutigen Konzept; wer gegen eine Datenbearbeitung vorgehen will, kann dies vom Zivilgericht verlangen. Das gilt auch für das Recht, eine Berichtigung von Personendaten zu verlangen (bisher Art. 5 DSG, neu Art. 4 Abs. 5 DSG und Art. 25 DSG). Den «Bestreitungsvermerk» gibt es weiterhin. Es wird jetzt aber auch festgehalten, dass die bestrittenen Daten nur noch eingeschränkt bearbeitet werden, was schon bisher möglich war, auch wenn dies nicht ausdrücklich im Gesetz vorgesehen war. Es wird in diesen Fällen eine Interessenabwägung stattfinden müssen; rechtlich handelt es sich um einen Anwendungsfall des Widerspruchs gegen eine Datenbearbeitung, der nur mit einer entsprechenden Rechtfertigung (nach Art. 13 DSG bzw. Art. 24 VE DSG) wie etwa einem überwiegenden privaten Interesse «übergangen» werden kann.

[Rz 69] Neu ist hingegen die Regelung, wonach im Falle einer Berichtigung, Löschung oder Vernichtung von Daten und in weiteren Fällen der Verantwortliche und Auftragsbearbeiter die Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtungen etc. mitteilen müssen, soweit dies nicht oder nur mit «unverhältnismässigem» Aufwand möglich ist (Art. 19 Bst. b VE DSG). Eine Begrenzung auf Fälle, in denen die betroffene Person ein schützenswertes Interesse hat, fehlt hingegen leider. Es ist nicht einmal erforderlich, dass die Berichtigung, Löschung oder Vernichtung auf einen Vorstoss der betroffenen Person zurückzuführen ist. Das kann zu absurden Verhältnissen führen, denn es gibt viele Gründe, warum Daten berichtigt, gelöscht oder vernichtet werden, ohne dass sich eine Nachinformation bisheriger Empfänger der Daten aufdrängt. Letztere benutzen die Daten möglicherweise gar nicht mehr. Oder eine Löschung erfolgt nicht, weil die Daten datenschutzwidrig bearbeitet wurden oder die betroffene Person dies verlangt hat, sondern weil sie der Inhaber selbst schlicht nicht mehr braucht. Das darf nicht eine Pflicht nach Art. 19 Bst. b VE DSG auslösen, sonst müsste jedes Unternehmen, das seine Archive und dergleichen bereinigt laufend prüfen, wem es die Daten schon einmal mitgeteilt hat und diese darüber informieren. Weil das schon ist im Ansatz unsinnig ist, kann es nicht sein, dass die Nachinformation lediglich wegen dem damit allenfalls verbundenen unverhältnismässigen Aufwand wegfällt. Art. 19 Bst. b VE DSG könnte zum Beispiel so eingeschränkt werden, dass sie nur zum Tragen kommen, wenn eine Person die Nachinformation aus berechtigten Gründen verlangt.

[Rz 70] Die DSGVO kennt eine ähnliche Regelung wie Art. 19 Bst. b VE DSG, doch geht der Vorentwurf auch bezüglich der mitzuteilenden Daten darüber hinaus,[67] als dass auch Verletzungen des Datenschutzes den Empfängern der davon betroffenen Daten mitgeteilt und somit offengelegt werden müssen. Das gilt paradoxerweise selbst dann, wenn die betroffenen Personen selbst darüber nicht informiert werden müssen. Aus der Regel geht auch nicht hervor, ob nur die melde-

66 Vgl. auch Postulat Schwaab 12.3152 und Erläuterungen VE DSG, S. 37.

67 Art. 19 DSGVO.

pflichtigen Datenschutzverletzungen gemeint sind, oder alle, wie es der Wortlaut suggeriert. So oder so ist nicht klar, welchen Sinn diese Pflicht haben soll. Sie ist überdies unverhältnismässig und greift ohne zwingenden Grund in die Privatsphäre der betroffenen Unternehmen ein.

[Rz 71] Man stelle sich zum Beispiel vor, dass in einem Unternehmen ein Mitarbeiter unbefugten Zugriff auf Daten nimmt, die das Unternehmen auch mit seinen Kunden teilt. Der Zugriff wird diesen als Datenschutzverletzung nach Art. 19 Bst. b VE DSG mitgeteilt werden müssen, obwohl er für diese Kunden ohne jede Relevanz ist, den Ruf der Firma aber schädigen wird. Ein anderes Beispiel wäre eine Zeitung, die im Zusammenhang mit der Berichterstattung über eine Person eine sie betreffende Datenschutzverletzung begeht. Nach der Regel von Art. 19 Bst. b VE DSG müsste die Zeitung diese Tatsache, sobald sie sie feststellt, allen Lesern des betroffenen Beitrags mitteilen, was technisch gesehen natürlich ohne Weiteres möglich ist. Tut sie dies nicht, können die betroffenen Mitarbeiter der Zeitung strafrechtlich verfolgt werden. Die Pflicht zur Mitteilung gilt zudem ungeachtet dessen, ob dies die betroffene Person oder andere Dritte in ihren Rechten verletzt.

## 9. Auch Daten verstorbener Personen geregelt

[Rz 72] Der Vorentwurf enthält mit Art. 12 VE DSG auch Bestimmungen zu Daten verstorbener Personen. Eine Regelung dieser Daten gibt es schon heute, allerdings ist sie erstens in Abs. 1 Abs. 7 VDSG versteckt und zweitens existiert für sie keine Rechtsgrundlage. Ohnehin gilt in der Schweiz der Grundsatz, dass die Persönlichkeit mit dem Tod endet[68], weshalb eine verstorbene Person auch keinen Datenschutz geniesst. Den Datenschutz geniessen allenfalls Personen im Umfeld der verstorbenen Person, die durch die Bearbeitung deren Daten ebenfalls betroffen sind. Die neue Regelung von Art. 12 VE DSG ist daher aus Sicht des Datenschutzes überflüssig. Dass es sie trotzdem gibt und ihr Regelungsgehalt über das bisherige Auskunftsrecht hinaus ausgebaut wird, ist die Folge einer politischen Intervention, welche Regelungen zum «digitalen Tod» in sozialen Medien verlangte.[69]

[Rz 73] Aus der Sicht der Praxis sind solche Zeitgeist-Regelungen unnötig und schädlich, da sie nur aufgrund eines sehr eng begrenzten, zum betreffenden Zeitpunkt gerade öffentlich diskutierten, aber meist nicht wirklich nachhaltig relevanten Anwendungsfalls hinaus verfasst werden. Problematisch sind solche Regelungen, weil sie aufgrund ihrer generell abstrakten Natur unzählige andere, nicht bedachte weitere Anwendungsfälle mitbetreffen und damit unkontrollierte und unüberlegte Nebenwirkungen haben. Das wird auch in diesem Fall so sein, da die Regelung keineswegs nur auf soziale Medien Anwendungen findet, sondern auf alle Unternehmen die Daten von natürlichen Personen bearbeiten.

[Rz 74] Verlangt ein einzelner Erbe, gleich in welcher Beziehung er zur verstorbenen Person steht, dass deren Daten gelöscht werden, soll sich das betroffene Unternehmen zum Beispiel nur auf überwiegende Interessen von Dritten oder der verstorbenen Person selbst berufen können, nicht aber etwa auf eigene überwiegende Interessen oder gesetzliche Pflichten, wie z.B. Aufbewahrungspflichten (Art. 12 Abs. 4 VE DSG). Damit hat der Erbe wesentlich mehr Rechte gegen einen Datenbearbeiter in der Hand als der Erblasser zu Lebzeiten, was keinen Sinn macht. Zudem bleibt

68 Art. 31 Abs. 1 ZGB.

69 Postulat Schwaab 14.3782 und Erläuterungen VE DSG, S. 38.

völlig im Dunkeln, ob und welche Interessen eine tote Person sachlogisch überhaupt haben kann. Konflikte unter den Erben regelt die Bestimmung ebenfalls in keiner Weise – sie sind naturgemäss vorprogrammiert. Interessant wird auch die Frage sein, wie der auskunftspflichtige Verantwortliche prüfen soll, ob eine Person eine faktische Lebensgemeinschaft mit der verstorbenen Person geführt hat.

[Rz 75] Durch die Universalsukzession der Vertragsverhältnisse mit den betreffenden sozialen Medien auf die Erbengemeinschaft und die weiteren Bestimmungen des anwendbaren Vertrags- und Erbrechts sowie der eigenen Persönlichkeitsrechte der Nachfahren wären die wesentlichen Rechtsfragen, die Sache des Gesetzgebers sind, hinreichend geklärt, oder dort zu klären und nicht im DSG. Erforderlich ist daher falls überhaupt nur eine moderate Bestimmung zum Auskunftsrecht; systematisch wäre es sinnvoller, sie mit der Revision des DSG ins ZGB aufzunehmen, wo sie hingehört, so zum Beispiel als neuen Art. $38^{bis}$ ZGB mit den Nachwirkungen der Ende der Persönlichkeit.

## 10. Massnahmen zur Sicherstellung des Datenschutzes

[Rz 76] Etliche der Bestimmungen des Vorentwurfs konkretisieren technische und organisatorische Massnahmen, die heute unter Art. 7 Abs. 1 DSG subsumiert werden könnten. Sie dienen der Gewährleistung des Datenschutzes, indem sie direkt oder indirekt auf die Einhaltung der Regelungen hinwirken.

[Rz 77] Die meisten dieser Bestimmungen wurden ins Gesetz genommen, um ein Zeichen zu setzen. Sie sind rechtlich an sich überflüssig, ergeben sie sich doch bereits aus einer korrekten Anwendung des Bearbeitungsgrundsatzes, wonach im Rahmen einer Datenbearbeitung jeweils angemessene (sprich: dem Risiko entsprechende) technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte (sprich: DSG-widrige) Datenbearbeitung zu verhindern.

[Rz 78] Dieser Grundsatz findet sich in Art. 11 VE DSG. Neu wird hierbei der (ungewollte) «Verlust» von Daten als Unterform der unbefugten Bearbeitung im Einklang mit der Praxis der EU gesondert aufgezählt; erfasst war er schon bisher. Es wird allerdings nicht nur dem Bundesrat überlassen, diesen Grundsatz zu konkretisieren. Art. 18 Abs. 1 VE DSG tut dies unter dem Titel «Datenschutz durch Technik» (neudeutsch: «*Privacy by Design*»), wobei im Grunde dasselbe gesagt wird wie in Art. 11 Abs. 1 VE DSG, mit dem einzigen Hinweis, dass die Massnahmen bereits ab dem Zeitpunkt der Planung der Datenbearbeitung zu treffen sind, was aber so oder so gilt, wenn solche Massnahmen im Rahmen einer Datenbearbeitung von Anfang an bestehen müssen.

[Rz 79] Art. 18 Abs. 2 VE DSG schreibt den Grundsatz «datenschutzfreundlicher Voreinstellungen» («*Privacy by Default*») vor, welcher vor allem Anbieter von Online-Diensten und -Apps zwingen soll, die Grundeinstellungen ihrer Dienste so zu programmieren, dass von den im Rahmen eines Dienstes angebotene Datenbearbeitungen standardmässig die am wenigsten weitgehende vorgesehen ist. Die Formulierung im Vorentwurf bringt dies nicht wirklich zum Ausdruck und ist sachlogisch unkorrekt, da es nicht um die Frage geht, ob mehr Daten als für einen bestimmten Verwendungszweck erforderlich bearbeitet werden sollen, sondern zu welchem Verwendungszweck die Daten standardmässig vorgesehen werden soll. Hier ist somit eine Überarbeitung der Formulierung nötig. Ohnehin wäre es aufgrund der Nähe zu Art. 11 VE DSG sinnvoll, die beiden Grundsätze in den Wortlaut von Art. 11 Abs. 1 VE DSG zu integrieren, was mit wenigen Worten möglich wäre.

[Rz 80] Dies gilt im Übrigen auch für die in Art. 19 Bst. a VE DSG aufgeführte Pflicht zur Dokumentation der Datenbearbeitungen, die einerseits eine organisatorische Massnahme im Sinne von Art. 11 VE DSG darstellt und andererseits der Datenschutzaufsicht dient. Unternehmen werden hier gespannt auf die Konkretisierung im Rahmen der Verordnung sein, da je nach Ausgestaltung der Dokumentationspflicht ein erheblicher Aufwand auf sie zukommt. Sinnvoll wäre eine Regelung, die jedenfalls nicht über das von Art. 30 DSGVO vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgeht, und eine Klarstellung, dass nur *regelmässige* Datenbearbeitungen in ein solches Inventar aufgenommen werden müssen, analog der heutigen Regelung von Art. 11a Abs. 3 DSG. Hinzu kommt, dass die meisten Unternehmen auch für die DSGVO nur *strukturierte* Datenbestände bzw. Datenbearbeitungen erfassen werden; eine solche Einschränkung erscheint aus Sicht der Praktikabilität und Möglichkeiten der Governance ebenfalls sinnvoll. Wird die Dokumentationspflicht zu breit oder absolut verstanden, muss jedes Schreiben einer E-Mail oder eines Briefs dokumentiert sein, weil sie jeweils eine Datenbearbeitung darstellen. Das wäre unsinnig. Es stellt sich vor diesem Hintergrund zudem die Frage, ob der gestrichene Begriff der Datensammlung nicht doch weiterhin benutzt werden sollte, um bezüglich gewisser Pflichten unter dem neuen DSG eine sinnvolle Beschränkung zu ermöglichen. Schliesslich wäre zu klären, dass mit Bezug auf die Dokumentation das Rad nicht neu erfunden werden muss und die Bestimmung keine eigenständige Dokumentation für Datenschutzzwecke erfordert, sondern es genügt, dass zum Beispiel auf bestehende Dokumentationen zurückgegriffen werden kann (z.B. ein Betriebshandbuch eines Systems) oder sich die Dokumentation sogar aus dem System selbst ergibt.

[Rz 81] Die in Art. 19 Bst. a VE DSG erwähnte Pflicht soll gemäss den Erläuterungen die Datenbearbeiter auch verpflichten, die Datenschutzverstösse im Sinne von Art. 17 VE DSG zu dokumentieren[70]. Hier kann auf die nachfolgenden Ausführungen zu diesem Thema verwiesen werden (vgl. Rz 93 ff. unten). Angesichts dem breiten Begriffsverständnis von Art. 17 VE DSG erscheint auch diese Dokumentation uferlos und ohne sichtbaren Mehrwert für den Datenschutz; hierbei ist zu beachten, dass diese Pflicht für jedes Unternehmen gilt, sei es noch so klein. Die DSGVO sieht eine solche Dokumentationspflicht zwar auch vor, geht aber von einem sehr viel engeren Verständnis der zu erfassenden Verstösse aus.

[Rz 82] Erstaunlicherweise keinen Eingang in die Vorlage gefunden haben Bestimmungen zum betrieblichen Datenschutzbeauftragten. Richtigerweise wird ein solcher nicht vorgeschrieben. Das war schon bisher nicht der Fall, und auch die DSGVO schreibt ihn für die meisten Betriebe nicht vor. Die Funktion des betrieblichen Datenschutzbeauftragten wäre aber ideal, um den EDÖB in gewissen Bereichen zu entlasten, wenn sichergestellt ist, dass eine solche Stelle über die nötigen Kompetenzen und das nötige Know-how verfügt. Es könnte zum Beispiel analog der bisherigen Regelung in Art. 11a DSG vorgesehen sein, dass die diversen Informations- und Meldepflichten wegfallen, soweit sie überhaupt beibehalten werden sollen, wenn ein Unternehmen selbst über eine solche Stelle verfügt; dies wäre ein erheblicher Anreiz zur Schaffung einer solchen Stelle, was wiederum der Datenschutz-Governance zugutekäme.

70 Erläuterungen VE DSG, S. 65.

## 11. Datenschutz-Folgenabschätzungen

[Rz 83] Ein neues Instrument zur Sicherstellung des Datenschutzes sind die «Datenschutz-Folgenabschätzungen» (*Privacy Impact Assessments*), welche Art. 16 VE DSG neu in allen Fällen vorschreibt, in welchen eine vorgesehene Datenbearbeitung «voraussichtlich zu einem erhöhten Risiko» für die Persönlichkeit der betroffenen Personen vorsieht. Eine solche Abklärung muss nicht zwingend umfangreich sein, wie die Erfahrung zeigt. Es geht im Wesentlichen darum, zunächst zu dokumentieren, wie die Datenbearbeitung vor sich gehen soll, was dabei schiefgehen bzw. negative Auswirkungen auf die betroffene Person haben kann, und welche Massnahmen zu ihrem Schutz vorgesehen sind, um diese Risiken und Auswirkungen auszugleichen (Abs. 2). Das mag auf einer Seite Platz finden. Das Ergebnis ist dem EDÖB mitzuteilen (Abs. 3), der dann etwaige Einwände innert einer Frist von drei Monaten nach Erhalt aller erforderlichen Informationen anmelden muss (Abs. 4).

[Rz 84] Auch die DSGVO schreibt solche Datenschutz-Folgenabschätzungen vor, und selbst im heutigen Schweizer Recht gibt es sie in den Kantonen teilweise schon[71]. Allerdings ist die im Vorentwurf vorgeschlagene Regelung in verschiedener Hinsicht problematisch. Erstens erscheint die Hürde für die Durchführung einer Abklärung sehr tief angesetzt. «Erhöhte» Risiken werden in der Praxis rasch gegeben sein, womit für fast alle Datenbearbeitungen vorab entsprechende Abklärungen durchgeführt werden müssen, mit den damit verbundenen Aufwänden und massiven Verzögerungen (dazu sogleich). Diesbezüglich beruhigen auch die Erläuterungen nicht, soll es doch schon genügen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann[72], was in sehr vielen Fällen der Fall sein wird. Die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling soll bereits Indiz für ein «erhöhtes» Risiko sein, ebenso die Übermittlung in Drittstaaten ohne angemessenen Datenschutz. Die Strafbewehrung der Bestimmung wird ein ihres dazu beitragen, dass selbst in Fällen, in denen an sich kein erhöhtes Risiko besteht, aus Angst vor Strafbarkeit ein entsprechendes Verfahren durchgeführt wird, inklusive Meldung an den EDÖB. So wäre es bei der jetzigen Ausgangslage nicht erstaunlich, wenn inskünftig jede Übermittlung in die USA, jedes Profiling und jede Bearbeitung von besonders schützenswerten Personendaten zu einer Datenschutz-Folgenabschätzung führt, was völlig übertrieben wäre. Der dafür erforderliche Aufwand für die Wirtschaft (und den EDÖB) wäre enorm, ohne dass für den Datenschutz wirklich etwas gewonnen wäre.

[Rz 85] Die EU verlangt im Gegensatz dazu entsprechende Abklärungen nur bei «hohen» Risiken. Hierbei ist zu berücksichtigen, dass ohnehin jedes Bearbeitungsprojekt geprüft werden muss, denn nur dadurch kann überhaupt ermittelt werden, ob es voraussichtlich zu erhöhten oder hohen Risiken führt. Wesentlich ist, dass die gesetzliche Pflicht zur Erstellung einer formalen, dokumentierten Abklärung auf das beschränkt wird, was wirklich zwingend nötig ist. Die Fälle, in welchen Unternehmen solche formalisierten Abklärungen tatsächlich vornehmen sollen, sollten zudem im Rahmen der Verordnung konkretisiert werden. Eine Ausnahme bietet sich zudem für Fälle an, in welchen das Gesetz ein Unternehmen die Datenbearbeitung vorgibt, auch wenn die konkrete Ausgestaltung natürlich Risiken mit sich bringen kann, die adressiert werden müssen. Solche Fälle sind jedoch nicht im Fokus von Art. 16 VE DSG; die damit verbundenen

71 Vgl. etwa die Vorabkontrolle gemäss § 10 des ZH-IDG, die erforderlich ist, wenn eine Datenbearbeitung «besondere Risiken» mit sich bringt.

72 Erläuterungen VE DSG, S. 61.

fallspezifischen Risiken müssen im Rahmen der jeweiligen Gesetzesvorgaben abgewogen werden und, soweit ein Unternehmen nur die gesetzlichen Vorgaben umsetzt, wird die Datenbearbeitung in der Regel in materieller Hinsicht datenschutzkonform nach Art. 24 Abs. 1 VE DSG gerechtfertigt sein.

[Rz 86] Unpassend erscheint weiter, dass der Vorentwurf die Pflicht zur Abklärung nicht nur dem Verantwortlichen auferlegt, wie dies die DSGVO tut, sondern auch dem Auftragsbearbeiter, obwohl dieser dazu regelmässig nicht in der Lage sein wird und es auch nicht seine Aufgabe ist. Natürlich kann der Verantwortliche eine solche Abklärung an seinen Auftragsbearbeiter delegieren, aber es bleibt schon von der Natur der Sache her eine Pflicht des Verantwortlichen.

[Rz 87] Die Meldepflicht gegenüber dem EDÖB und die ihm eingeräumte Frist zur Bearbeitung ist schliesslich praxisfern und wird die Datenbearbeiter massiv behindern. Ein grosses Pharmaunternehmen aus Basel führt beispielsweise jedes Jahr weit über hundert solche Datenschutz-Folgeabschätzungen durch. Würden sie vom EDÖB ernsthaft geprüft, müsste er alleine für dieses Unternehmen eine eigene Person abstellen. Das wird er nicht und das kann auch nicht sinnvoll sein. Selbst die DSGVO ist weniger streng: Sie verlangt eine Konsultation der Aufsichtsbehörde nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm ergriffenen Schutzmassnahmen ein hohes Risiko der Verletzung der Persönlichkeit der betroffenen Personen verbleibt.[73]

[Rz 88] Die dem EDÖB gewährte Frist zur Beurteilung ist überdies viel zu lange: In der EU muss eine Behörde innert acht Wochen handeln, falls sie sich gegen eine Bearbeitung ausspricht, und die Frist kann nur in komplexen Fällen um sechs Wochen verlängert werden.[74] In der Schweiz soll der EDÖB standardmässig drei Monate Zeit haben, mit der Möglichkeit, durch das Einfordern weiterer Information die Frist jedes Mal von neuem beginnen zu lassen.

[Rz 89] Wird der vorgeschlagene Art. 16 VE DSG tatsächlich so umgesetzt, bedeutet dies für Unternehmen, dass sie bei jedem Projekt, das eine Datenbearbeitung beinhaltet und diese nicht problemlos erscheint, einen Vorlauf von vielen Monaten einplanen müssen, um nach ihrer eigenen Abklärung auch etwaigen Anforderungen des EDÖB gerecht zu werden. Dies wird die Wirtschaft völlig unnötig lähmen und erhebliche Kosten verschlingen. Mag eine Wartezeit in gewissen Projekten noch handhabbar sein, wird sie in anderen Fällen zu erheblichen Schwierigkeiten führen. Man stelle sich zum Beispiel ein ausländisches Gerichtsverfahren oder eine Anfrage einer ausländischen Aufsichtsbehörde vor, für welches bzw. für welche innert Wochen gewisse Unterlagen geliefert werden müssen, die auch Angaben von Mitarbeitern enthalten. Nach der vorgeschlagenen Regelung wäre dies nicht mehr oder nicht sinnvoll möglich. Solche Fälle werden fast immer erhöhte Risiken mit sich bringen, müssten also dem EDÖB vorgelegt werden. Ebenso wird es aber nicht möglich sein, die Monate, die er zur Klärung der möglichen Massnahmen braucht, abzuwarten. Das Unternehmen wird sich entscheiden müssen, dem ausländischen Recht zu folgen und möglicherweise Schweizer Recht zu verletzen bzw. die Konsultation des EDÖB nutzlos werden zu lassen, oder umgekehrt. Dabei sieht die Regelung keine Ausnahmen vor, und dies nicht einmal für den Fall, in welchem alle betroffenen Personen mit der Datenbearbeitung einverstanden sind.

[Rz 90] Auch für den EDÖB wird diese Regelung im Ergebnis nicht angenehm werden. Wird ihm ein Projekt vorgelegt, wird er sich damit zwangsläufig auseinandersetzen müssen, denn tut er es

73 Art. 36 Abs. 1 DSGVO.

74 Art. 36 Abs. 2 DSGVO.

nicht und stellt sich das Projekt später als datenschutzrechtlich problematisch heraus, wird er dafür möglicherweise nicht rechtlich, aber öffentlich und politisch zur Verantwortung gezogen werden, weil er nicht rechtzeitig interveniert hat bzw. keine Einwände äusserte. Dies wird daher auch seinerseits erhebliche Ressourcen binden, über die er aber nicht verfügt bzw. die an anderer Stelle eingespart werden müssen. Sinnvoller wäre, dieses Konsultationsverfahren auf die wirklich heiklen Fälle zu beschränken.

[Rz 91] Zu klären ist weiter die Frage, unter welchen Umständen Datenschutz-Folgenabschätzungen im Rahmen von bestehenden Datenbearbeitungen vorzunehmen bzw. zu wiederholen oder aufzufrischen sind, falls überhaupt. Denn Risiken können sich verändern, die Umstände und Datenbearbeitungen ebenfalls. Der Wortlaut von Art. 16 VE DSG ist diesbezüglich nicht klar, impliziert aber aufgrund von Abs. 1 und 4, dass eine *formalisierte* Abklärung nur jeweils bei der Erstaufnahme einer Datenbearbeitung durchzuführen ist. Dies wäre in der Botschaft in diesem Sinne klarzustellen.

[Rz 92] Im Zusammenhang mit Art. 16 VE DSG sei noch erwähnt, dass diese auf ein Risiko «für die Persönlichkeit oder die Grundrechte» der betroffenen Personen abstellt. Diese Formulierung ist verwirrend. Zwar dient das DSG schon bisher gemäss Art. 1 nicht nur dem Schutz der Persönlichkeit, sondern auch den Grundrechten der betroffenen Personen, doch gilt letzteres nur mit Bezug auf die Datenbearbeitungen durch Behörden im engeren Sinn. Private sind normalerweise nicht zur Wahrung der Grundrechte verpflichtet; in ihrem Bereich dient das DSG – und damit die Datenschutz-Folgenabschätzung – ausschliesslich dem Schutz der Persönlichkeit der betroffenen Personen. Der Verweis auf die «Grundrechte» sollte daher sinnvollerweise überall gestrichen werden. Er hat keinen Mehrwert.

## 12. Data Breach Notifications

[Rz 93] Was ursprünglich in den USA erfunden wurde, soll es nun auch in der Schweiz geben: *Data Breach Notifications*. Es geht um die Meldung von Datenschutzverstössen, einschliesslich Datenverlust. Eine solche Pflicht bestand bisher nicht, jedenfalls nicht in formalisierter Form. Schon nach heutigem Recht kann es erforderlich sein, im Falle einer Datenschutzverletzung gewisse Sofortmassnahmen wie etwa die Sperrung von abhanden gekommenen Kreditkartendaten auszuführen. Auch die Mitteilung an den EDÖB kann in bestimmten Fällen ratsam sein. Neu soll jedoch *jeder* Datenschutzverstoss dem EDÖB «unverzüglich» gemeldet werden, es sei denn, dieser führe «voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person» (Art. 17 Abs. 1 VE DSG).

[Rz 94] Diese Bestimmung ist insofern bemerkenswert, als sie deutlich über die entsprechende Bestimmung der DSGVO hinausgeht, und zwar ohne ersichtlichen Grund. In der EU wird eine Meldung dann erforderlich sein, wenn im Rahmen einer Datenbearbeitung festgestellt wird, dass eine getroffene Sicherheitsmassnahme verletzt wurde (z.B. ein Einbruch in ein Computernetz oder ein Mitarbeiter, der weisungswidrig Daten auf einen privaten Memorystick kopiert) und diese Verletzung zu einem Bruch oder Verlust des Gewahrsams an den Daten führt.

[Rz 95] In der Schweiz soll die Meldepflicht hingegen jede Datenbearbeitung erfassen, die gegen das DSG verstösst, also z.B. eine zweckentfremdete oder unverhältnismässige Nutzung von Daten oder eine Datenbeschaffung, die in nicht transparenter Weise erfolgt. Solche Fälle kommen in jedem Betrieb erfahrungsgemäss jeden Tag vor. Die Ausnahme, in welchem Fall nicht gemeldet

werden muss, ist dabei schon so formuliert, dass sie im Falle einer Datenschutzverletzung nicht gegeben sein kann, stellt doch eine unbefugte Datenbearbeitung immer eine Persönlichkeitsverletzung dar.

[Rz 96] Selbst wenn nur die etwas schwereren Fälle gemeldet werden müssen, wird die Schweizer Regelung ungleich viel mehr Fälle erfassen, als gemäss der DSGVO der Aufsichtsbehörde gemeldet werden müssen. Sachliche Gründe gibt es dafür nicht. Der logische Grund für die Meldepflicht ist das Bedürfnis, der Aufsichtsbehörde die Möglichkeit zu geben, in den Umgang mit einer Datenschutzverletzung aktiv einzugreifen und zum Beispiel die Benachrichtigung der betroffenen Personen zu verlangen (vgl. Abs. 2). Müsste aber tatsächlich wie vorgesehen gemeldet werden und halten sich die Betriebe auch daran, würde der EDÖB jeden Tag mit einer Vielzahl von Meldungen geflutet werden. Die Idee der Regelung wäre durch sie selbst vereitelt.

[Rz 97] Die im Vorentwurf vorgesehene Meldepflicht bringt aber auch die Mitarbeiter in einem Unternehmen in eine Zwickmühle und sorgt für völlig unverhältnismässigen Druck und letztlich eine Angstkultur: Stellt zum Beispiel der interne Datenschutzverantwortliche eine Datenschutzverletzung im eigenen Betrieb fest und könnte sie zu einem Risiko für die betroffenen Personen führen, muss er sie dem EDÖB melden und damit die dafür verantwortlichen Personen «ans Messer» liefern: Je nach Verstoss werden sie dafür strafrechtlich verfolgt werden müssen[75], da der EDÖB seinerseits eine Anzeigepflicht hat (dazu Rz 119 unten). Tut der Datenschutzverantwortliche dies nicht, muss er selbst mit strafrechtlicher Verfolgung rechnen (Art. 50 Abs. 2 Bst. e VE DSG). Dies wird für ihn, der darauf angewiesen ist, dass andere Mitarbeiter mit ihm offen über Datenschutzprobleme sprechen, eine unhaltbare Situation sein. Doch auch dort, wo der Datenschutzverantwortliche selbst für den Datenschutzverstoss (mit-)verantwortlich ist, sind Konflikte vorprogrammiert (Stichwort *nemo tenetur*, vgl. Rz 125 unten).

[Rz 98] Die Meldepflicht ist daher mindestens auf das Niveau der DSGVO zu reduzieren, und selbst diese geht weit. Auch die strafrechtlichen Sanktionen sind zu überdenken bzw. zu prüfen, inwiefern eine Meldung möglicherweise sogar vor Strafe schützt, um einen möglichst offenen Umgang mit solchen Meldungen zu fördern. Sinnvoll erscheint eine Regelung, in welcher zudem nur Fälle gemeldet werden müssen, die eine Vielzahl von Personen betreffen, da sich ein Eingreifen der Aufsichtsbehörde nur dann wirklich rechtfertigt. Versendet ein Spital zum Beispiel einen heiklen Befund versehentlich an den falschen Patienten, ist das zwar eine gewichtige Persönlichkeitsverletzung, aber weshalb es in einem solchen Fall zum Schutz des betroffenen Patienten nötig sein sollte, dass der EDÖB eingeschaltet wird, ist nicht ersichtlich. Eine Pflicht, die betroffene Person direkt zu informieren, wenn es zum Schutz der betroffenen Person erforderlich ist, ist in Abs. 2 bereits vorgesehen.[76]

[Rz 99] Die Meldepflicht sollte zudem in zeitlicher Hinsicht relativiert werden. Statt einer «unverzüglichen» Meldung sollte eine Meldung ohne unnötigen Verzug stattfinden. Denn zwischen dem Erkennen eines Verstosses und dem Zeitpunkt, an welchem genügend Informationen vorliegen, damit sich der EDÖB ein vernünftiges Bild machen kann, vergeht normalerweise einige Zeit. Es bringt gar nichts, dem EDÖB vorab eine Mitteilung machen zu müssen, dass ein Unternehmen

75 So zum Beispiel die Mitarbeiter der Informatik, welche es unterlassen haben, die zum Schutz der Daten notwendigen Massnahmen zu treffen, was bei vorsätzlicher und fahrlässiger Begehung strafbar sein soll (Art. 51 VE DSG).

76 Der zweite Fall («oder der Beauftragte es verlangt») ist irreführend formuliert und überflüssig. Ist es zum Schutz der betroffenen Person nicht erforderlich, gibt es auch keinen Grund, warum der EDÖB eine Information verlangen sollte.

einen Datenschutzverstoss entdeckt hat, aber noch nicht wirklich sagen kann, was passiert ist, warum und welche Massnahmen es trifft. Der EDÖB ist ohnehin in einer viel schlechteren Lage zu beurteilen, was an Massnahmen sinnvollerweise zu ergreifen ist als das betroffene Unternehmen.

[Rz 100] In Abs. 4 wird schliesslich dem Auftragsbearbeiter die Pflicht auferlegt, den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung zu informieren, wobei nicht klar wird, ob diese Pflicht nur Verstösse in seinem Verantwortungsbereich betrifft oder auch Verstösse, die der Auftragsbearbeiter seitens des Verantwortlichen wahrnimmt. Sachlogisch muss ersteres gelten. Anders als Abs. 1 sieht Abs. 4 allerdings keine Informationspflicht im Falle von Datenverlust vor. Korrekterweise ist der Hinweis auf den Datenverlust zu streichen, denn wenn ein Datenverlust nicht zugleich eine Datenschutzverletzung darstellt, gibt es in der Sache keinen Grund, diesen melden zu müssen.

## 13. Auftragsdatenbearbeitung

[Rz 101] Im Bereich der Auftragsdatenbearbeitung, die neu in Art. 7 VE DSG geregelt ist, soll sich mit drei Ausnahmen nicht viel ändern:

[Rz 102] Erstens wird nun ausdrücklich festgehalten, dass sich der Verantwortliche vergewissern muss, dass der Auftraggeber nicht nur in der Lage ist, die Datensicherheit zu gewährleisten, wie dies schon bisher ausdrücklich verlangt wurde, sondern neu auch, dass die Rechte der betroffenen Personen gewährleistet sind (Abs. 2). Was dies genau bedeutet, ist nicht wirklich klar, ist die Gewährleistung der Rechte der betroffenen Personen doch primär die Aufgabe des Verantwortlichen. Handelt es sich wie oft beim Auftragsbearbeiter um eine im Hintergrund agierende Person (wie z.B. ein Outsourcing-Dienstleister), tritt sie gegenüber den betroffenen Personen nicht auf und ist auch nicht deren Ansprechpartner. Richtigerweise müsste also sichergestellt sein, dass der Auftragsbearbeiter das in seinem Bereich Erforderliche tut, damit der *Verantwortliche* die Rechte der betroffenen Personen gewährleisten kann. So wird ein Verantwortlicher prüfen müssen, ob der Auftragsbearbeiter ihm den für einen Auskunftsanspruch erforderlichen Datenzugang gewährleistet oder dass er Datenlöschungen, die der Verantwortliche durchführen muss, ausführen kann.

[Rz 103] Zweitens dürfte der Mindestinhalt der Verträge zwischen Verantwortlichem und Auftragsbearbeiter neu indirekt durch die Verordnung zum DSG konkretisiert werden. Es ist zu vermuten, dass dies analog der Regelung der DSGVO erfolgt. Dies wird bedeuten, dass auf das Inkrafttreten des neuen DSG kurzfristig alle Verträge mit Auftragsbearbeitern überprüft werden müssen. Die Kompetenzdelegation in Abs. 2 ist jedoch problematisch: Sie spricht nicht von einer Konkretisierung der in Art. 7 VE DSG geregelten Grundsätze, sondern von «weiteren» Pflichten, was fallengelassen werden sollte: Es gibt keinen Anlass, dem Bundesrat das Recht einzuräumen, für die Auftragsdatenbearbeitung *weitere* Pflichten vorzusehen, als sie das DSG ohnehin schon vorsieht, und diese gehen schon jetzt zu weit. Eine solche Regelung ist überdies aus rechtsstaatlicher Sicht heikel.

[Rz 104] Drittens wird ein Auftragsbearbeiter weitere Auftragsbearbeiter neu nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen beiziehen dürfen (Abs. 3). Diese Regelung entspricht derjenigen der DSGVO, wobei dort klargestellt wird, dass auch eine generelle Einwilligung möglich ist, die noch keinen Bezug auf die einzelnen Unter-Auftragsbearbeiter nimmt. Zu

denken ist etwa an eine generische Klausel im Vertrag zwischen Verantwortlichem und Auftraggeber, in welchem die Zustimmung pauschal erteilt wird. In der DSGVO wird für diesen Fall verlangt, dass der Verantwortliche vor dem Beizug eines bestimmten Auftragsbearbeiters den Verantwortlichen über diesen informiert und ihm ein Vetorecht gibt. Dies sollte an sich auch für die Schweiz gelten, geht aus der neuen Bestimmung in Abs. 3 aber nicht hervor. Da dieses Vetorecht eine sehr spezielle Regelung darstellt, wäre es angezeigt, darauf hinzuweisen; bisher findet sich ein Hinweis lediglich in den Erläuterungen.[77] Ungenau ist auch der Hinweis auf die Notwendigkeit, dass die Zustimmung schriftlich erfolgt, denn wenn es sich dabei um Schriftlichkeit im Sinne von Art. 13 OR handelt[78], was normalerweise der Fall ist, wenn sich aus dem Gesetz nichts Weiteres ergibt, werden z.B. Online-Verträge mit Cloud- und Internet-Providern nicht mehr möglich sein, da diese regelmässig Unterauftragnehmer haben. Wesentlich kann nicht sein, dass die Zustimmung schriftlich im Sinne des OR erfolgt. Wesentlich ist, dass sie in dokumentierter Weise erfolgt, also ein Nachweis durch Text möglich ist.

[Rz 105] Aus der Regel des Zustimmungsvorbehalts in Abs. 3 ergibt sich implizit im Übrigen auch, dass es weiterhin erlaubt sein wird, dass es genügt, wenn die Verträge mit Unterbeauftragten nur mit dem Auftragsbearbeiter abgeschlossen werden, also keine direkte Vertragsbeziehung zum Verantwortlichen erforderlich ist.[79] Das ist in der Praxis ein wichtiger Aspekt und gilt so unter bestehendem Recht und auch in der EU. In diesen Fällen wird dann der Auftragsbearbeiter die Rolle des Verantwortlichen gegenüber dem Unterbeauftragten übernehmen. Bei diesem Fall zeigt sich auch, wie durchdacht und differenziert die bisherige Terminologie des Schweizer Rechts war: Es unterschied die Rolle der Inhaberschaft der Datensammlung (bzw. neu der Funktion des Verantwortlichen) von jener des Auftraggebers, da ein Auftraggeber nicht zwingend der (in letzter Instanz) Verantwortliche ist.

## 14. Brisant, aber kreativ: Die «Empfehlungen der guten Praxis»

[Rz 106] Die sicherlich kreativste aber auch rechtsstaatlich «speziellste» Neuerung des Vorentwurfs ist das Konzept der «Empfehlungen der guten Praxis» in Art. 8 und 9 VE-DSG. Die Idee ist in jedem Fall begrüssenswert; sie war auch schon im Vorfeld diskutiert worden und ist auch keine Schweizer Erfindung. Das österreichische Recht kennt sie zum Beispiel schon. Es adressiert das Grundproblem des DSG, das mit seinem Konzept «Prinzipien statt Regeln» zwar sehr flexibel ist und so bestens für die jeweiligen Umstände richtig angewandt werden kann, dadurch aber für den nicht bewanderten Leser zu wenig konkret ist und damit gewisse Rechtsunsicherheiten schafft: Er weiss in der Praxis oft nicht, was genau erlaubt ist und was nicht. Dem wurde bisher mit «Soft Law» begegnet. Neu soll es möglich sein, bestimmte Verhaltensweisen vom EDÖB als datenschutzkonform absegnen zu lassen (Art. 8 Abs. 2 VE DSG). Der EDÖB soll aber auch selbst «Empfehlungen» abgeben, wie sich bestimmte Dinge datenschutzkonform tun lassen (Abs. 1). Diese Empfehlungen sollen keine «*best practice*» sein, sondern lediglich «*good practice*», und in

77 Erläuterungen VE DSG, S. 52.

78 Welche Bestimmung in der Regel eine handschriftliche Unterschrift auf einem festen Träger erfordert.

79 Eine «Zustimmung» braucht es sachlogisch nur in Fällen, in welchen die zustimmende Partei selbst nicht Vertragspartei ist.

Art. 9 Abs. 2 VE DSG wird richtigerweise betont, dass sie in keiner Weise zwingend sind und der Datenschutz auch auf andere Weise eingehalten werden kann.

[Rz 107] Der Clou findet sich aber in Art. 9 Abs. 1 VE DSG, wonach die Einhaltung einer vom EDÖB verfassten oder genehmigten «Empfehlung der guten Praxis» für einen Verantwortlichen bedeutet, dass er die damit konkretisierten Bestimmungen des DSG befolgt hat (warum dies nicht auch für einen Auftragsbearbeiter gelten sollte, ist nicht ersichtlich; dies dürfte ein Versehen sein). Es handelt sich rechtstechnisch um eine Fiktion, die auch für die Gerichte bindend sein wird. Spannend ist dabei, dass in keiner Weise vorgesehen ist, wie oder dass der Erlass oder die Genehmigung einer Empfehlung einer rechtsstaatlichen Kontrolle unterliegen soll. Der EDÖB kann bezüglich seiner eigenen Empfehlungen gemäss Vorentwurf tun und lassen, was er will.

[Rz 108] Die Empfehlungen der guten Praxis qualifizieren nicht als Verfügungen und sind daher auch nicht als solche anfechtbar. Verfügungscharakter wird zwar Genehmigung einer Fremdempfehlung haben: Weist der EDÖB eine beispielsweise von einem Branchenverband vorgelegte Empfehlung als ungenügend ab, wird er auf Verlangen des Verbands eine beschwerdefähige Verfügung ausstellen müssen, gegen die der Verband vorgehen kann. Nach Art. 8 Abs. 2 VE DSG besteht ein Anspruch auf Genehmigung, wenn die vorgelegte Empfehlung mit den Vorschriften des DSG «vereinbar» ist. Sind umgekehrt die betroffenen Personen, deren Daten im Einklang mit einer solchen Empfehlung der guten Praxis bearbeitet werden, mit ihr nicht einverstanden, werden sie sich höchstens indirekt wehren können. Wie das gehen soll, ist aber völlig unklar, denn der Vorentwurf sieht hierzu nichts vor. Es ist in der Tat erstaunlich, dass die damit zusammenhängenden Fragen auch in den Erläuterungen nicht diskutiert werden. Dabei kann die Wirkung einer Empfehlung der guten Praxis massiv sein: Ist sie zu Unrecht genehmigt oder erlassen worden, beraubt sie die betroffenen Personen aufgrund der Fiktion der Gesetzmässigkeit der Datenbearbeitung ihrer gesetzlichen Rechte. Dem Autor ist ein vergleichbares Instrument des Schweizer Rechts bisher nicht bekannt. Hier sind eingehende Überlegungen zum Rechtsschutz erforderlich. Dazu gehört zum Beispiel auch eine Befristung der Empfehlungen der guten Praxis, deren Überarbeitung oder deren gerichtliche Überprüfung. Denkbar ist zum Beispiel ein System analog den Angemessenheitsentscheidungen der Europäischen Kommission, die zwar von den nationalen Gerichten nicht überprüft werden können, die Beurteilung eines Einzelfalls jedoch vorbehalten bleibt. So könnte beispielsweise festgehalten werden, dass die Einhaltung der Empfehlung der guten Praxis nicht eine Fiktion der Datenschutzkonformität zur Folge hat, sondern lediglich eine widerlegbare Vermutung.

[Rz 109] Schon vor diesem Hintergrund dürfte die Regelung, wonach der EDÖB alleine über Ausgestaltung oder Genehmigung einer solchen Empfehlung der guten Praxis bestimmen kann, dazu führen, dass er an solche Empfehlungen einen strengen, übergesetzlichen Massstab anlegen wird. Hinzu kommt, dass dem EDÖB inoffiziell die Rolle des «Beschützers» betroffener Personen und eine solche Empfehlung einen generell abstrakten Charakter haben muss und daher die Berücksichtigung der Umstände im Einzelfall gar nicht möglich ist. Empfehlungen der guten Praxis werden daher zweifellos nicht das Minimum dessen umschreiben, was zur Einhaltung des DSG getan werden muss, sondern letztlich trotz allem eine «beste Praxis» sein, nicht nur eine «gute Praxis». Ihre Gefahr wird darin liegen, dass sie von Gerichten möglicherweise als Richtschnur für die korrekte Umsetzung des DSG herangezogen werden und sie daher bewirken, dass diese das DSG im Ergebnis zu Lasten der Interessen der Datenbearbeiter anwenden, wie dies vom Gesetzgeber an sich nicht beabsichtigt war.

[Rz 110] Weiter stellt sich nebst den bereits angeführten Punkten die Frage, ob es nicht erforderlich ist, ein im Gegensatz zum EDÖB *neutrales*, von ihm unabhängiges Gremium über die Geltung von Empfehlungen der guten Praxis bestimmen zu lassen, wie zum Beispiel eine Kommission, in welcher insbesondere auch Vertreter aus der Praxis einsitzen. Denn Praxiswissen ist gerade in diesem Bereich von zentraler Bedeutung, fehlt dem EDÖB aber erfahrungsgemäss oftmals. Eine solche Vorgehensweise würde den EDÖB zudem personell entlasten und wäre vergleichsweise kostengünstig umzusetzen; dagegen spricht, dass eine solche Kommission ein de facto politisches Gremium wäre, während es vorliegend wichtig ist, Entscheide auf einer Sachebene zu fällen.

[Rz 111] Ein möglicher Ansatz wäre auch, dem EDÖB gar nicht zu gestatten, eigene Empfehlungen der guten Praxis erlassen zu dürfen, sondern nur solche zu genehmigen, die ihm von privater Seite vorgelegt werden. Das Instrument hätte dann stärker den Charakter einer Selbstregulierung. Diese Lösung würde auch dem in breiten Kreisen vorhandene Unbehagen begegnen, dass der EDÖB über seine eigenen Empfehlungen der guten Praxis strengere Anforderungen an ein datenschutzkonformes Verhalten einführt, als das Gesetz es verlangt. In der Vergangenheit wurden seitens des EDÖB immer wieder Regelungen als geltendes Recht vertreten, die klar keine gesetzliche Grundlage haben.[80] Mindestens jedoch sollte der EDÖB verpflichtet werden, die betroffenen Verkehrskreise vor dem Erlass einer Empfehlung der guten Praxis zu konsultieren bzw. eine gerichtliche Überprüfung solcher Empfehlungen durch diese vorgesehen werden, analog dem heute gegen unzulässige öffentliche Behauptungen des EDÖB möglichen Vorgehen gegen Realakte.

## 15. Aufsicht und Sanktionen: Deutlich härtere Gangart

[Rz 112] Die mit Sicherheit am meisten beachtete neue Regelung des Vorentwurfs sind die Sanktionen, die neu eingeführt werden. Heute kennt das DSG keine nennenswerten Sanktionen; sanktioniert werden gewisse Verhaltensweisen im Zusammenhang mit dem Auskunftsrecht, die vorsätzliche Unterlassung der besonderen Informationspflicht bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen und der Kooperations-, Registrier- und Meldepflichten gegenüber dem EDÖB. Sie führten in der Praxis zu so gut wie keinen Verurteilungen.

[Rz 113] Dass sich dies mit dem Vorentwurf ändern würde, war klar, verlangt doch auch die revidierte Konvention 108 die Einführung von «Administrativsanktionen» im Falle einer Datenbearbeitung, welche die Vorgaben der Konvention verletzt.[81] Vor diesem Hintergrund war erwartet worden, dass der Vorentwurf für Datenschutzverletzungen künftig Verwaltungssanktionen einführt, wie sie auch schon diverse andere Gesetze wie etwa das Fernmeldegesetz oder Kartellgesetzt kennen. Diese sehen Bussen von bis zu zehn Prozent des Jahresumsatzes vor. Die DSGVO setzt ebenfalls hauptsächlich auf Verwaltungssanktionen, die dort bis zu vier Prozent des Jahresumsatzes entsprechen dürfen, allerdings bemessen am weltweiten Umsatz des Unternehmens oder der Unternehmensgruppe, dies je nach Lesart der DSGVO.[82]

---

80 So beispielsweise, dass die Bearbeitung von Persönlichkeitsprofilen eine Einwilligung erfordert. Das Gesetz verlangt nur bei der *Bekanntgabe* von Persönlichkeitsprofilen an Dritten eine Einwilligung *oder* einen anderen Rechtfertigungsgrund.

81 Art. 12$^{bis}$ Abs. 2 Bst. c der revidierten Konvention 108 (Entwurf Stand September 2016).

82 Art. 83 DSGVO.

[Rz 114] Es kam anders: Art. 50 ff. VE DSG setzt primär auf private, strafrechtliche Sanktionen gegen die einzelnen, in eine Verletzung des DSG involvierten Organe und Mitarbeiter. Der Vorentwurf geht somit auch hier über die DSGVO und das, was von der Konvention 108 verlangt wird, hinaus. Der Bussenrahmen beträgt CHF 500'000 für die vorsätzliche Begehung der einzelnen Delikte, erfasst aber mit Bussen von bis zu CHF 250'000 auch fahrlässige Datenschutzverstösse. Ein fahrlässiger Verstoss gegen das DSG kann somit gleich massiv geahndet werden wie die fahrlässige Verletzung des Bankgeheimnisses. Zum Vergleich: Die fahrlässige Verletzung des Amts-, Anwalts- oder Arztgeheimnisses ist nicht strafbar.[83]Immerhin: Anstiftung und Gehilfenschaft sind bei Übertretungen wie hier nicht strafbar.

[Rz 115] Art. 53 VE DSG sieht zwar vor, dass von der Ermittlung der strafbaren Person in einem Betrieb abgesehen werden kann, wenn die Busse CHF 100'000 nicht überschreiten wird; in diesem Falle wird das Unternehmen gebüsst. Der einzelnen Person, die sich durch eine Handlung möglicherweise strafbar macht, wird diese Regelung jedoch kaum den nötigen Komfort geben, da ihre Strafbarkeit von einem entsprechenden Entscheid der ermittelnden Behörde abhängt. Da die Sanktionen strafrechtlicher Natur sind, muss damit gerechnet werden, dass sie weder versichert werden können, noch vom Unternehmen für den Gebüssten bezahlt werden dürfen, da dies als eine strafbare Verfolgungsbegünstigung qualifiziert werden könnte.[84]

[Rz 116] Der persönliche, strafrechtliche Charakter der Sanktionen ist unverhältnismässig und nicht zielführend. Speziell diejenigen Personen, die wie etwa betriebliche Datenschutzverantwortliche in ihrer Tätigkeit für den Datenschutz an sich geschützt und gestärkt werden sollten, werden durch die Schaffung eines persönlichen Strafbarkeitsrisikos unnötig unter Druck gesetzt und exponiert (vgl. z.B. Rz 97 oben). Mitarbeiter in den Unternehmen werden sich hüten, in strafrechtlich bedrohten Datenschutzfragen selbst Entscheide zu treffen, ohne sich über externen Rechtsrat durch Spezialisten abgesichert zu haben, was zu einer unnötigen Verteuerung der Datenbearbeitung führt und dazu, dass die Möglichkeiten des DSG zur Datenbearbeitung nicht mehr ausgeschöpft werden. Damit aber kommt der vom Gesetzgeber gewollte Ausgleich zwischen den Interessen der betroffenen Personen und der Datenbearbeiter nicht mehr zum Tragen. Die ersten Reaktionen auf den Vorentwurf lassen vermuten, dass die gegenwärtig vorgeschlagenen strafrechtlichen Sanktionen politisch wenig Chancen haben werden.

[Rz 117] Das gilt ganz besonders für die Strafbarkeit von fahrlässigen Verstössen gegen das DSG. Solche Verstösse sind natürlich nicht hinzunehmen, aber eine Kriminalisierung der einzelnen Mitarbeiter ist stossend, zumal die Delikte in den meisten Fällen «nur» in der Verletzung *flankierender* Massnahmen wie etwa eine unterlassene Datenschutz-Folgenabschätzung oder Dokumentation der Datenbearbeitung bestehen, durch welche die betroffenen Personen zunächst nicht wirklich in ihrer Privatsphäre verletzt sind. Pikanterweise sind jene Fälle, in denen die Persönlichkeit einer betroffenen Person tatsächlich verletzt werden, nicht unter Strafe gestellt. Gebüsst wird nicht derjenige, der Personendaten bewusst zweckwidrig oder unverhältnismässig verwendet, sondern derjenige, der vergisst, diese Datenschutzverletzung dem EDÖB zu melden. Das kann nicht sein.

---

83 Art. 320 f. StGB.

84 Art. 305 StGB; allerdings ist darauf hinzuweisen, dass diese Frage im Falle der Bezahlung einer Geldbusse durch einen Dritten in der Lehre umstritten ist (gegen das Vorliegen einer Begünstigung: Vera Delnon/Bernhard Rüdy, Basler Kommentar, 3. Auflage, Art. 305 StGB, N 20, m.w.H.).

[Rz 118] Einige Stimmen vertreten gar die Ansicht, dass es gar keine Sanktionen braucht, was aus Sicht des Datenschutzes sicherlich stimmt (die Nichteinhaltung einer Verfügung des EDÖB könnte bereits mit der bestehenden Regelung von Art. 292 des Schweizerischen Strafgesetzbuches StGB sanktioniert werden), aber für manche im Widerspruch zum Wortlaut der Konvention 108 steht. Es kann immerhin vertreten werden, dass der Begriff der Administrativsanktion nicht zwingend eine Geldbusse erfordert; auch ein Bearbeitungsverbot könne eine solche sein, wird argumentiert. Allerdings dürften die realpolitischen Chancen, dass das revidierte DSG keine finanziellen Sanktionen enthält, sehr gering sein.

[Rz 119] Wer nach den Gründen der scharfen Regelung im Vorentwurf forscht, dem wird rasch klar, dass sie rein opportunistischer Natur sind: Dem EDÖB soll offenkundig nicht die mit der Sanktionierung von Datenschutzverstössen verbundene (Arbeits-)Last auferlegt werden. Durch eine strafrechtliche Sanktionierung können die Fälle an die Kantone abgeschoben werden.[85] Kommt diese Regelung durch, werden die kantonalen Staatsanwaltschaften künftig auch einen Datenschutzjuristen einstellen müssen, um die betreffenden Fälle zu untersuchen und abzuurteilen. Dies zeigt zugleich, wie ineffizient diese Regelung ist: Zwar ist es denkbar, dass ein Datenschutzverstoss von einer betroffenen Person direkt zur Anzeige gebracht und untersucht wird. Der Regelfall wird jedoch sein, dass ein Fall zunächst vom EDÖB untersucht werden wird (dazu Rz 126 unten). Dieser soll dann im Falle eines strafrechtlich relevanten Verhaltens Anzeige erstatten; Art. 45 VE DSG verpflichtet ihn dazu. Derselbe Fall wird dann von der zuständigen Strafbehörde nochmals untersucht werden müssen. Dies ist auch zwingend erforderlich, da nur so die strafprozessualen Rechte der Beschuldigten gewahrt werden können. Dass sich die Strafbehörden mangels eigener Datenschutzerfahrung wohl auf die Einschätzung des EDÖB abstützen werden, macht die Sache rechtsstaatlich nicht besser.

[Rz 120] Der gewählte Weg der strafrechtlichen Sanktion zwingt auch zur Befassung mit dem strafrechtlichen Bestimmtheitsgebot.[86] Dies dürfte mit ein Grund dafür sein, dass vor allem formelle Pflichten bzw. Massnahmen zur Datenschutz-Governance und –Aufsicht strafrechtlich sanktioniert werden und nicht datenschutzwidrige Datenbearbeitungen selbst. Der gewählte Ansatz ändert jedoch nichts daran, dass viele der sanktionierten Bestimmungen viel zu offen formuliert sind, dass es für den Rechtsunterworfenen schwierig sein wird zu verstehen, was er genau tun darf und was nicht. Dies wird dazu führen, dass er entweder weniger weit geht, als er dies an sich tun können sollte, oder es wird schwierig werden, ihn strafrechtlich zu belangen, weil das DSG das sanktionierte Verhalten zuwenig bestimmt umschreibt.

[Rz 121] Inhaltlich werden die Strafregelungen ebenfalls überarbeitet werden müssen. So sind ein Teil der Delikte nur auf Antrag strafbar, doch ist unklar, wer in solchen Fällen antragsberechtigt sein soll. Beispiele sind die Pflicht zur Dokumentation von Datenbearbeitungen oder die Durchführung einer Datenschutz-Folgenabschätzung (Art. 51 VE DSG). Antragsberechtigt sind jedoch nur Personen, die durch eine solche Unterlassung verletzt werden.[87] Durch die Unterlassung einer Dokumentation oder Folgenabschätzung wird jedoch niemand verletzt, jedenfalls nicht direkt oder höchstens in sehr speziellen Konstellationen. Die Bestimmung bleibt damit toter Buchstabe. Der EDÖB kann ebenfalls nicht sanktionieren, und auch eine etwaige Strafanzeige seinerseits wäre unbeachtlich.

85 Art. 54 VE DSG, welche Bestimmung jedoch überflüssig ist.

86 Art. 1 StGB.

87 Art. 30 Abs. 1 StGB.

[Rz 122] Die Strafbestimmungen in Art. 50 f. VE DSG sind nicht die einzigen, die eingeführt oder angepasst werden sollen:

- Das heute in Art. 35 DSG geregelte «kleine» Berufsgeheimnis, das bisher nur besonders schützenswerte Personendaten und Persönlichkeitsprofile schützte, wird ausgebaut und zu einem allgemeinen Berufsgeheimnis für jeden erweitert, der für die Zwecke seines Berufes geheime Personendaten bearbeiten muss oder solche schlicht zu «kommerziellen Zwecken» bearbeitet. Statt den Verrat nur mit Busse zu sanktionieren, sieht die Norm neu auf Antrag eine Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe vor. Die Bestimmung steht damit dem «grossen» Berufsgeheimnis für Anwälte, Ärzte und Geistliche[88] in nichts mehr nach. Im Gegenteil: Eine Befreiung von der Geheimnispflicht durch eine etwaige Aufsichtsbehörde ist nicht vorgesehen. Die Auswirkungen dieser Anpassung sind noch unklar. Gegenüber Art. 162 StGB grenzt sich die Bestimmung dadurch ab, dass sie nicht nur Geschäftsgeheimnisse, sondern auch «private» Geheimnisse schützt. Weiter kann die Frage gestellt werden, ob die Norm nur dann angewandt werden kann, wenn mindestens implizit zwischen Geheimnisherr und Geheimnisträger eine vertragliche Geheimhaltungspflicht besteht, wie sie Art. 162 StGB verlangt oder zum Beispiel auch das Bankgeheimnis.[89] Soll die Anwendung nicht uferlos werden, wird verlangt werden müssen, dass die Information nicht nur geheim ist, sondern der Geheimnisherr auch eine berechtigte, in einem Vertrag oder sonstigem Verhalten oder Übung begründete Erwartung hat, dass der Geheimnisträger sie auch geheim halten wird. Doch selbst dann hat die Bestimmung einige Sprengkraft, da sie sehr viele Personen, die sich dem gar nicht bewusst sein werden und dies auch nicht erwarten, neu einem strafrechtlich sanktionierten Berufsgeheimnis unterstellt, weil argumentiert wird, dass sie implizit eine Geheimhaltungspflicht haben. So gehen die Erläuterungen offenbar davon aus, dass künftig auch Online-Händler und Betreiber sozialer Netzwerke mit Bezug auf die Daten ihrer Kunden unter diese Regelung fallen und sie etwa zur Anwendung gelangen kann, wenn diese für Marketingzwecke unberechtigterweise verkauft werden.[90] Es wird nicht lange dauern bis argumentiert werden wird, dass eine vorsätzlich datenschutzwidrige Bekanntgabe von nicht jedermann zugänglichen Personendaten in einem Geschäftsbetrieb immer auch eine Verletzung der beruflichen Schweigepflicht darstellt und daher mit bis zu drei Jahren Freiheitsstrafe sanktioniert werden kann. Das erscheint nicht angemessen. Die mit der Anpassung angestrebte Anlehnung an Art. 321 StGB leuchtet nur auf den ersten Blick ein: In den in Art. 321 StGB erfassten Berufen ist es für alle Beteiligten klar, dass Kundendaten grundsätzlich vertraulich zu behandeln sind. Bei einem Online-Shop oder einem sozialen Netzwerk ist das eben nicht der Fall; die beiden Anwendungsvoraussetzungen von Art. 52 VE DSG lösen dieses Problem nicht, da sie beliebig viele Fälle erfassen. Hier wäre entscheidend, dass nur solche Daten der beruflichen Schweigepflicht unterliegen, für welche eine Schweigepflicht unabhängig von Art. 52 VE DSG klar besteht, denn sonst unterliegt so gut wie jeder Berufstätige einer strafrechtlich sanktionierten Schweigepflicht, was unsinnig ist. Es stellt sich die Frage, warum der bisherige Art. 35 DSG nicht einfach beibehalten wird; einen guten Grund für seine Anpassung ist jedenfalls nicht ersichtlich und ein diesbezüglicher Leidensdruck besteht auch nicht wirklich.

88 Art. 321 StGB.

89 Art. 47 BankG.

90 Erläuterungen VE DSG, S. 86.

- Art. 179$^{novies}$ StGB soll ebenfalls ausgeweitet werden und stellt neu jeden auf Antrag unter Strafe, der «unbefugt» Personendaten beschafft, «die nicht für jedermann zugänglich sind». Die Strafandrohung ist mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe deutlich höher als die Bussen, die für sonstige Datenschutzverletzungen vorgesehen sind. Allerdings ist nicht klar, inwiefern die mit der neuen Formulierung zu erfassenden Delikte von den sonstigen Datenschutzverletzungen abgrenzen sollen. Die bisherige Regelung kam nur dann zum Tragen, wenn unbefugt nicht frei zugängliche besonders schützenswerte Personendaten oder Persönlichkeitsprofile aus einer Datensammlung beschafft wurden. Gemeint waren damit allerdings Datendiebstähle aus gesicherten Systemen und Räumen, und nicht eine blosse Verletzung des Datenschutzes, indem eine Person etwa unter Missachtung des Transparenz- oder Verhältnismässigkeitsgrundsatzes Daten erhob, was ja nach Wortlaut ebenfalls erfasst wäre und den Anwendungsbereich der Norm massiv erweitert hätte. Dies scheint trotz einer geringfügigen Anpassung des Wortlauts (neu «für jedermann zugänglich» statt wie heute «frei zugänglich») nicht der Fall zu sein. Die Erläuterungen sprechen jedenfalls lediglich darüber, dass die von der Bestimmung erfassten Datenkategorien erweitert werden sollen.[91] Die «Unbefugtheit» meint somit nicht unbefugt im Sinne einer Verletzung des DSG (wie etwa in Art. 11 VE DSG), sondern ohne Befugnis des für die Daten Verantwortlichen.[92]
- In Art. 179$^{decies}$ StGB neu eingeführt werden soll schliesslich eine Bestimmung zur strafrechtlichen Ahndung des Identitätsmissbrauchs.[93] Er soll dann bestraft werden können, wenn die Identität einer anderen Person dazu verwendet wird, dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen. Diese Bestimmung erscheint sinnvoll, da gegen ein solches Verhalten bisher meist nur zivilrechtlich vorgegangen werden konnte, was wiederum regelmässig daran scheiterte, dass die Identität des Täters ohne strafprozessuale Mittel nicht ermittelt werden konnte.

[Rz 123] Nebst Strafbestimmungen sollen auch die Rechte des EDÖB erweitert werden. Das bisherige System der Sachverhaltsabklärungen, Empfehlungen und Klagen vor Bundesverwaltungsgericht wird, obwohl es gut funktioniert, abgeschafft. Neu soll der EDÖB die Kompetenz erhalten, gegen Datenbearbeiter verwaltungsverfahrensrechtliche Untersuchungen durchzuführen (Art. 41 VE DSG) und gegen diese Verfügungen zu erlassen, sei es in Form von vorsorglichen Massnahmen (Art. 42 VE DSG), sei es, um eine Datenbearbeitung anzupassen, sie zu stoppen, einschliesslich der Bekanntgabe ins Ausland, oder um Daten zu vernichten (Art. 43 VE DSG). Der EDÖB soll offenbar sogar die Kompetenz erhalten, gegen eine Bekanntgabe ins Ausland selbst dann vorzugehen, wenn sie nicht gegen das DSG, sondern gegen ein anderes Gesetz verstösst; was dies bedeuten soll, wird aber nicht näher erläutert.[94]

[Rz 124] Problematisch ist in diesem Zusammenhang, dass Beschwerden gegen vorsorgliche Massnahmen *per se* keine aufschiebende Wirkung haben sollen (Art. 44 Abs. 3 VE DSG). Hierbei ist zu berücksichtigen, dass eine vorsorglich verfügte Einstellung oder Anpassung einer Datenbearbeitung gerade im Bereich der automatisierten Datenbearbeitung massive Kosten bzw. Schäden zur Folge haben kann, die der EDÖB regelmässig nicht einschätzen können wird. Solange der Staat bzw. der EDÖB für diese nicht aufkommt, muss ein Unternehmen die Möglichkeit haben, sich

91 Erläuterungen VE DSG, S. 93.

92 David Rosenthal, Handkommentar DSG, Zürich 2008, Art. 179$^{novies}$ StGB, N 17.

93 Diese Bestimmung geht zurück auf die Motion Comte 14.3288.

94 Erläuterungen VE DSG, S. 80, mit Verweis auf Art. 12 Abs. 2 des Entwurfs der revidierten Konvention 108.

vor einer unabhängigen Instanz gegen ein unverhältnismässiges Vorpreschen des EDÖB wehren zu können. Das bisherige System, dass der EDÖB solche Massnahmen vom Bundesverwaltungsgericht beantragen musste, hat sich bestens bewährt (und gezeigt, dass der EDÖB gewisse vorsorgliche Massnahmen auch unberechtigt verlangt hat[95]).

[Rz 125] Das Verfahren richtet sich neu nach dem Verwaltungsverfahrensgesetz. Gemäss Vorentwurf soll der EDÖB das Recht haben, ohne Vorankündigung Hausdurchsuchungen durchzuführen und sich Zugang zu allen notwendigen Daten und Information zu verschaffen, muss das untersuchte Unternehmen aber vorgängig erfolglos zur Mitwirkung angehalten haben (Art. 41 Abs. 3 VE DSG). Wie das im Einzelnen vor sich gehen soll, bleibt unklar. Nicht wirklich diskutiert sind auch so heikle Fragen wie der Grundsatz *nemo tenetur* – das Recht zu Vorwürfen gegen die eigene Person zu Schweigen bzw. sich nicht selbst belasten zu müssen –, die sich angesichts der Pflicht zur Meldung von Datenschutzverstössen und den strafrechtlichen Konsequenzen akzentuiert stellen.

[Rz 126] Der EDÖB kann jederzeit ein Verfahren eröffnen, wenn Anzeichen bestehen, dass gegen das DSG verstossen wird; es muss nicht mehr eine grössere Zahl von Personen betroffen sein. Eine Pflicht zur Untersuchung besteht allerdings nicht, auch nicht im Falle einer Anzeige einer betroffenen Person. Immerhin muss der EDÖB diese über sein Vorgehen und das Ergebnis einer allfälligen Untersuchung informieren (Art. 41 Abs. 5 VE DSG); Partei ist sie nicht (Art. 44 Abs. 2 VE DSG), aber es steht ihr selbstverständlich offen, gestützt auf das ihr mitgeteilte Ergebnis (und weiteren Informationen, die sie über ein Gesuch nach Öffentlichkeitsgesetz erhält) gegen den Verantwortlichen zivilrechtlich vorzugehen. Diese neuen Bestimmungen sind aufgrund der Vorgaben der revidierten Konvention 108 und der politischen Stimmung erwartet worden. Viele Beobachter gehen jedoch auch davon aus, dass die Neuerungen dem Datenschutz nicht dienen werden: Zwar erhält der EDÖB mehr und schärfere Instrumente zur Aufsicht in die Hand, doch damit verbunden wird ebenso der Aufwand, den er für die entsprechenden Verfahren betreiben muss, deutlich steigen. Da jedenfalls bei der heutigen politischen Grosswetterlage nicht davon auszugehen ist, dass ihm hierfür mehr Mittel zur Verfügung stehen werden, wird er im Ergebnis weniger Fälle durchführen können. Immerhin soll ihm weiterhin das Recht zustehen, auch ausserhalb eines formellen Untersuchungsverfahrens zu überprüfen, ob ein Unternehmen (oder eine Behörde) die Datenschutzvorschriften einhält (Art. 41 Abs. 4 VE DSG). Obwohl in diesen Fällen kein Zwang zur Kooperation besteht, ist ein Widerstand seitens der betroffenen Unternehmen kaum zu erwarten.

## 16. Und wo bleiben die Übergangsregelungen?

[Rz 127] Schon bei der letzten Revision des DSG im Jahre 2008 stellten sich hinsichtlich der Übergangsregelungen etliche Fragen. Angesichts der noch sehr viel zahlreicheren Neuerungen, die der Vorentwurf vorsieht, erstaunt es daher, dass die Übergangsbestimmungen in Art. 59 VE DSG so mager ausgefallen sind.

95 So im Fall Moneyhouse im Sommer 2012, in welchem eine superprovisorische Sperrung des Dienstes kurze Zeit danach wieder aufgehoben wurde (vgl. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-45545.html).

[Rz 128] Zwei Jahre Zeit wird gewährt für die Erstellung der Dokumentation der zum Zeitpunkt des Inkrafttretens des revidierten DSG bereits bestehenden Datenbearbeitungen, zur diesbezüglichen Einführung des «*Privacy by Default*» und «*Privacy by Design*» und eines Verfahrens zur Datenschutz-Folgenabschätzung. Warum selbiges zum Beispiel nicht auch für ein Verfahren zur Meldung von Datenschutzverstössen gelten soll, bleibt unklar. Es fehlen auch Übergangsregelung für andere wichtige Punkte wie zum Beispiel die neuen Informations- und Auskunftspflichten, automatisierten Einzelentscheiden und Verträge mit Auftragsbearbeitern.

[Rz 129] Die einfachste Lösung wird daher sein, für die Umsetzung des revidierten DSG eine generelle Umsetzungsfrist von zwei Jahren vorzusehen. Zwar steht die Schweiz unter einem gewissen Druck der EU, ihr Datenschutzrecht anzupassen. Entscheidend wird jedoch sein, dass das Parlament das DSG revidiert, und nicht, wann genau es in Kraft tritt. Überdies hat die EU für die DSGVO ebenfalls eine Umsetzungsfrist von zwei Jahren vorgesehen, und zwar für alle Bestimmungen.

## 17. Abgrenzung zur DSGVO

[Rz 130] Viele Schweizer Unternehmen sehen sich heute nicht nur mit den Anforderungen eines revidierten DSG konfrontiert, sondern werden auch in den Geltungsbereich der DSGVO fallen. Dies ist nach Art. 3 DSGVO zum Beispiel dann der Fall, wenn sie Daten von Personen in der EU bearbeiten, weil sie diesen dort Produkte oder Dienstleistungen anbieten oder weil sie deren Verhalten analysieren, oder wenn sie deren Daten durch einen Auftragsbearbeiter in der EU (z.B. einen Cloud-Provider) bearbeiten lassen. Damit unterstehen diese Unternehmen zugleich auch der Aufsicht der nationalen EU-Datenschutzbehörden, die zwar nach Art. 55 Abs. 1 DSGVO nur jeweils für ihr «Hoheitsgebiet» zuständig sind, dieser Begriff aber gemäss den Erwägungen der DSGVO extraterritorial zu interpretieren ist.[96] Dies bedeutet für viele Schweizer Unternehmen, die Daten von Personen in der EU bearbeiten, dass sie inskünftig sowohl der Datenschutzaufsicht der Schweiz als auch aller von der Datenbearbeitung betroffenen Mitgliedstaaten der EU (und des EWR) unterstehen.[97] Dies wird zu einer massiven administrativen Zusatzbelastung für Schweizer Unternehmen führen, und überdies zu zahlreichen Rechtsunsicherheiten, da die DSGVO mit Bezug auf ihre Geltung für Unternehmen ausserhalb des Territoriums der EU unsorgfältig redigiert und nicht durchdacht ist.[98] Die Aufsichtstätigkeit der nationalen Datenschutzbehörden der EU-Mitgliedsstaaten auf Schweizer Hoheitsgebiet stellt wiederum die Schweizer Souveränität in Frage und birgt auch für daran mitwirkende Schweizer Unternehmen ein Risiko der Strafbarkeit nach Art. 271 StGB. Die Situation ist also mit anderen Worten konfus und verfahren.

[Rz 131] Vor diesem Hintergrund besteht dringender Abstimmungsbedarf zwischen der offiziellen Schweiz und der EU. Informelle Kontakte diesbezüglich bestehen bereits, und auch die Politik hat den Handlungsbedarf bereits erkannt. Eine Motion «Gegen Doppelspurigkeiten im

96 Erwägung 122 DSGVO.

97 Das Konzept des *One-Stop-Shop* gemäss Art. 56 DSGVO steht für Unternehmen ausserhalb der EU nicht zur Verfügung (vgl. dazu die «Guidelines for identifying a controller or processor's lead supervisory authority» der Artikel-29-Datenschutz-Arbeitsgruppe, WP 244, S. 7).

98 So ist zum Beispiel nicht klar, ob sich ein Schweizer Unternehmen auf Schweizer Recht zur Rechtfertigung einer Datenbearbeitung im Sinne von Art. 6 Abs. 1 Bst. c DSGVO berufen kann; gemäss Art. 6 Abs. 3 DSGVO scheint dies nicht der Fall zu sein, was jedoch zu unbilligen Ergebnissen führt.

Datenschutz»[99] wurde bereits im September 2016 eingereicht und vom Bundesrat zur Annahme empfohlen[100]; der Nationalrat ist dem im Dezember 2016 bereits gefolgt. Im besten Fall kommen die Behörden der beiden Rechtsordnungen überein, dass die (verwaltungsrechtliche) Aufsicht auf dem jeweiligen Hoheitsgebiet alleine Sache der jeweils nationalen Behörde ist, die sie nach ihrem eigenen Recht umsetzt. In diesem Fall wären aufsichtsrechtlich für Datenbearbeitungen durch Unternehmen in der Schweiz einzig der EDÖB zuständig, der sie nach DSG beurteilen würde. Auch die Informations- und Genehmigungspflichten würden für diese Unternehmen nur gegenüber ihm gelten; Schweizer Unternehmen müssten beispielsweise eine Datenschutzverletzung nur ihm und nicht auch allen betroffenen Datenschutzaufsichtsbehörden der jeweiligen EU-Mitgliedsstaaten mitteilen, und zwar nach den Vorgaben des DSG, nicht der DSGVO. Der Informationsfluss zwischen dem EDÖB und den Datenschutzbehörden der EU wäre über die im Vorentwurf ebenfalls vorgesehenen Bestimmungen zur Amtshilfe sichergestellt. Der zivilrechtliche Rechtsschutz bliebe jedoch unberührt, d.h. ein betroffener EU-Bürger könnte auch gegen ein Schweizer Unternehmen gestützt auf DSGVO vorgehen.[101] Dieser Rechtsschutz spielt in der Praxis jedoch eine untergeordnete Rolle.

[Rz 132] Es bleibt zu hoffen, dass die Bundesverwaltung die Gespräche mit der EU möglichst rasch auch offiziell aufnimmt. Zwar gibt es vereinzelt Stimmen, die der Ansicht sind, ein solches Vorgehen habe ohnehin keine Chance, weil die Schweiz gegenüber der EU keine Forderungen stellen könne. Die Realität in der EU zeigt jedoch, dass die EU ebenso an einer Abstimmung mit der Schweiz interessiert ist wie umgekehrt, da mit der Datenschutzaufsicht auch erhebliche Kosten verbunden sind. Kann die Datenschutzaufsicht über Unternehmen mit Sitz in der Schweiz faktisch an den EDÖB «delegiert» werden, kommt dies den einzelnen nationalen Aufsichtsbehörden entgegen, jedenfalls solange die Schweiz über vergleichbare Datenschutzregelungen verfügt und sie ihre Rechte bei Bedarf auf dem Weg der Amtshilfe durchsetzen können, was beides der Fall ist oder noch sein wird. Umgekehrt ist es politisch undenkbar, dass die Schweiz es zulässt, dass EU-Datenschutzbehörden eigene Zwangsmassnahmen nach eigenem EU-Recht durch den EDÖB auf Schweizer Territorium vollziehen lassen oder sogar direkt gegen Unternehmen in der Schweiz durchsetzen.[102] Die britische Regierung wird im Rahmen des BREXIT ähnliche Gespräche führen. Art. 50 Bst. a DSGVO sieht die Kompetenz zur Entwicklung solcher Mechanismen der internationalen Zusammenarbeit zur wirksamen Durchsetzung des Datenschutzes für die Europäische Kommission und die nationalen Aufsichtsbehörden im Übrigen bereits vor.

---

99 Motion Fiala 16.3752.

100 Wenngleich die Begründung des Bundesrats inhaltlich fehlerhaft ist, da sie die Erwägung 122 der DSGVO übersieht. Der Bundesrat geht noch davon aus, dass die EU-Aufsichtsbehörden keine Zuständigkeit für Aktivitäten auf dem Territorium der Schweiz beanspruchen, was falsch ist.

101 Bereits der heutige Art. 139 des Bundesgesetzes über das Internationale Privatrecht (IPRG) gibt einer betroffenen Person weitreichende Wahlrechte mit Bezug auf das Datenschutzrecht, welches auf ihren Fall anwendbar sein soll. Die extraterritoriale Anwendbarkeit, welche Art. 3 Abs. 2 DSGVO neu vorsieht, kennt die Schweiz damit schon lange. Es stellt sich freilich die Frage, ob es sinnvoll wäre, im Zuge der Revision des DSG auch hier gewisse Einschränkungen vorzunehmen und beispielsweise festzuhalten, dass ein ausländischer Erfolgsort (und damit die Anwendbarkeit von ausländischem Datenschutzrecht) nicht allen damit begründet werden kann, dass die Daten im betreffenden Land gespeichert werden. Dies würde beitragen, dass auf Schweizer Unternehmen nicht schon deshalb die DSGVO zur Anwendung kommen könnte, weil sie einen Cloud-Provider in der EU benutzen.

102 Die im Vorentwurf vorgeschlagene Amtshilfebestimmung in Art. 47 VE DSG bleibt diesbezüglich vage. Eine direkte Durchsetzung wäre eine Verletzung von Art. 271 StGB.

## 18. Schlussbemerkungen

[Rz 133] Im Vorentwurf für ein totalrevidiertes DSG steckt wesentlich mehr verborgen, als es auf den ersten Blick den Anschein macht. Positiv zu vermerken ist, dass die Schweiz der bewährten Tradition, mit Prinzipien statt ausformulierten Regeln zu arbeiten, treu bleiben will. Die Bestimmungen des allgemeinen Teils und des Teils für die Bearbeitung durch Privatpersonen beansprucht neu zwar 25 statt bisher 15 Artikel, doch ist das Gesetzeswerk dennoch erfreulich schlank und kein Vergleich zu den 99, teils furchtbar kompliziert und langwierig verfassten Artikeln der DSGVO.

[Rz 134] Der Vorentwurf erweckt zudem den Eindruck, dass das Bundesamt für Justiz im Datenschutz keine Revolution, sondern eine Evolution suchte mit dem primären Ziel, die Revision der Konvention 108 des Europarats nachzuvollziehen und die Adäquanz der Schweiz im Verhältnis zur EU weiterhin sicherzustellen[103]. Unsinnige Bestimmungen der DSGVO wie etwa jene der Datenportabilität[104] wurden daher zum Glück (vorerst) nicht übernommen, und auch sonst zeigt der Vorentwurf eine gesunde Distanz zur Rechtsetzung in der EU. Denn manches, was diese in der DSGVO umgesetzt hat, ist nicht wirklich durchdacht, und im Bereich der Datenbearbeitung durch Private ist die Schweiz jedenfalls nicht verpflichtet, die Regelungen der DSGVO zu übernehmen. Daher soll bei der Auslegung des DSG richtigerweise nicht einfach die Auslegung der DSGVO herangezogen werden.

[Rz 135] Bei näherer Betrachtung zeigt der Vorentwurf allerdings gewichtige Schwächen, die eine deutliche Überarbeitung erfordern werden. Dies erstaunt etwas, zumal die Vorlage im Rahmen der Ämterkonsultation intensiv kommentiert worden ist, was wohl der Grund für die mehrmonatige Verzögerung des Vorentwurfs ist. Trotz allem macht er einen unausgegorenen, praxisfremden Eindruck. Es entsteht der Anschein, dass mehr Zeit darin investiert worden ist, dem EDÖB genug Spielraum zu verschaffen als die Frage der Praktikabilität und der Auswirkungen auf die Unternehmen zu prüfen, die die neuen Vorgaben umzusetzen haben werden.

[Rz 136] Einige der Mängel sind in diesem Beitrag angesprochen. In etlichen Punkten geht der Vorentwurf zudem ohne guten Grund über die Anforderungen der DSGVO hinaus, auch wenn dies womöglich lediglich Versehen sind oder mit dem heutigen DSG zusammenhängt[105]. Ein solches «Swiss Finish» sollte es aber so oder so nicht geben. Die Wirtschaft wird durch parallele Anwendbarkeit von DSG und DSGVO ohnehin schwer belastet werden. Es sollte ihr daher die Compliance nicht mit einem DSG, das teilweise über die DSGVO hinausgeht, noch schwerer und kostspieliger gemacht werden, als sie in diesem Bereich ohnehin sein wird. In diesen Bereichen wird die Vorlage bei der Erarbeitung der Botschaft hoffentlich zurückgebunden werden.

[Rz 137] Auch wenn ein «Swiss Finish» aus politischen Gründen kaum Chancen haben wird, kommt auf die Schweizer Wirtschaft mit dem revidierten DSG einiges an Mehrarbeit zu. Das betrifft sowohl die Datenschutz-Governance, also die betriebsinternen Massnahmen zur Sicherstellung des Datenschutzes, als auch die Interaktion mit den betroffenen Personen, namentlich was die neuen und stark erweiterten Informations- und Auskunftspflichten betrifft. Dies wird

103 Erläuterungen VE DSG, S. 5 und 32.

104 Art. 20 DSGVO.

105 Dass z.B. auch manuelles Profiling erfasst wird, dürfte darin begründet sein, dass der Begriff den heutigen Begriff des Persönlichkeitsprofils ablöst, das ebenfalls manuell oder automatisiert entstehen kann.

insbesondere auch KMU treffen, die bisher kaum in diesen Bereich investiert haben und die dafür erforderlichen Prozesse und Dokumentationen erst noch schaffen müssen.

[Rz 138] Ob die Revision die Datenschutz-Aufsicht und die Durchsetzung des DSG ebenfalls stärken werden, ist hingegen eine andere Frage. Auf dem Papier wird der EDÖB durch die Verfügungskompetenz und die ausgebauten Untersuchungsmöglichkeiten zweifellos mehr Rechte haben. Die neuen Verfahren werden sein Wirken allerdings auch sehr viel komplizierter machen und von ihm mehr Aufwand abverlangen. Da jedoch bezweifelt werden darf, dass ihm die Politik mehr Mittel in die Hand geben wird, kann es durchaus sein, dass die Datenschutzaufsicht im Ergebnis künftig weniger bewerkstelligen kann, als sie es heute tut. Ob das im Sinne des Erfinders ist, ist allerdings eine andere Frage. Vom revidierten DSG werden vor allem die Datenschutzspezialisten, Sicherheitsexperten und Anwälte profitieren – jedenfalls jene, die sich angesichts der Strafbestimmungen noch trauen, in diesem Minenfeld zu beraten.

---

David Rosenthal, Lic. iur., Konsulent, Homburger AG, Zürich, Lehrbeauftragter ETH Zürich und Universität Basel; der Autor dankt Barbara Kaiser und Djamila Batache für die Unterstützung und insbesondere die sehr fruchtbaren Diskussionen zum Begriff der «Ausdrücklichkeit» einer Einwilligung.

## Amstutz Jonas BJ

**Von:** Eva Thelisson <evathelisson@protonmail.com>
**Gesendet:** Dienstag, 11. April 2017 18:34
**An:** Dubois Camille BJ; Amstutz Jonas BJ
**Betreff:** Commentaires avant-projet de révision de LPD
**Anlagen:** Commentaires .pdf

Chère Madame,

Veuillez trouver en annexe mes commentaires à l'avant-projet de révision de la loi fédérale sur la protection des données.

Meilleurs messages
Eva Thelisson
Doctorante en Droit, Université de Fribourg

**Commentaires relatifs à l'avant-projet de LPD dans le cadre de la procédure de consultation**

**Appréciation générale**

L'avant-projet semble remplir dans l'ensemble les dispositions de la Convention STE-108, du Règlement Général sur la protection des données (UE) 2016/679 et de la Directive européenne (UE) 2016/680 relative à la protection des personnes physiques.

**Enjeux principaux** :

- La reconnaissance du principe d'adéquation de la législation suisse sur la protection des données par la Commission Européenne et la ratification par la Suisse du protocole d'amendement de la Convention STE-108.
- Le respect des engagements pris par la Suisse dans le cadre de l'accord Schengen conclu avec l'UE.
- La défense du droit fondamental à la protection des données (art. 13 Constitution et art. 8 de la Charte des droits fondamentaux).
- La défense de la compétitivité des entreprises suisses et de l'innovation technologique à l'ère digitale.

La donnée bénéficie d'un double statut : il s'agit à la fois d'un bien marchand, valorisable sur un marché en fonction de l'offre et de la demande et d'un droit fondamental à la protection. Ces deux aspects doivent être **également** pris en considération par la loi cadre sur la protection des données.

Nous avons constaté que certaines dispositions importantes du Règlement Général à la Protection des Données (RGPD) n'avaient pas été intégrées dans l'avant-projet. Nous vous proposons de tenir compte des éléments suivants :

1. **Délégué à la protection des données (DPO) :** Le RGPD suggère la désignation d'un **Délégué à la Protection des Données** (DPO, articles 37 à 39 RGPD) et rend cette désignation obligatoire dans un certain nombre de cas (« pour tous les organismes publics et lors de traitements à grande échelle de données sensibles ou de données de suivi de personnes de matière régulière et systématique » (art. 37 RGPD). La fonction de DPO n'apparaît pas à ce jour dans l'avant-projet de révision de la LPD. Le DPO est appelé à jouer un rôle important dans les organisations des pays membres de l'UE après le 25 mai 2018. Il a pour mission de définir et de mettre en œuvre la gouvernance effective des données à caractère personnel dans son organisation. Le DPO doit identifier les différentes catégories de données (structurées et non structurées), effectuer une cartographie des flux de données à caractère personnel, documenter les traitements de données à caractère personnel et apporter les preuves de la conformité de son organisation lors d'un audit.
   Il serait utile de préciser la formation, les missions et la responsabilité du DPO. Il serait également important de définir les notions de « grande échelle » et de « suivi régulier et systématique ». Le DPO va jouer un rôle essentiel au sein des organisations, notamment du fait de son indépendance.

2. **Indépendance de l'autorité de contrôle :** Bien qu'il bénéficie d'un nouveau pouvoir d'enquête et d'un pouvoir de décision contraignant, le Préposé fédéral à la protection des données ne dispose d'aucun budget autonome et d'aucun pouvoir de sanction administrative, selon l'avant-projet. Cela ne reflète pas les dispositions du RGPD.

   La prévision d'un ou deux postes supplémentaires semble également bien faible au regard des enjeux. Un effort considérable devra être entrepris en matière de sensibilisation et d'éducation de la population suisse face aux enjeux de la protection des données à l'ère digitale. Chaque application technologique présente en effet un modèle d'affaire fondé sur la donnée : Big Data, Intelligence Artificielle, Deep Mining, Deep Analytic, Machine Learning, objets connectés par internet, Blockchain, Smartphones, Smart Cities, Smart Homes, véhicules autonomes, réseaux sociaux, robots et drones, Cloud Computing, convergence des NBIC.

   Le renforcement des pouvoirs du Préposé Fédéral à la protection des données et l'octroi d'une réelle indépendance budgétaire, renforceraient la sécurité juridique et la position de la Suisse envers la Commission européenne en plus de donner au préposé fédéral les moyens de remplir sa mission de manière effective.

3. **Sanctions administratives :** En cas de non-conformité, les sanctions dans l'UE pourront atteindre jusqu'à 20 millions d'Euros et jusqu'à 4% du chiffre d'affaire annuel mondial (le montant le plus élevé étant retenu). Dans un objectif de sécurité juridique, nous proposons de conserver les mêmes sanctions que le Règlement général sur la protection des données. La sanction devrait également être proportionnelle au chiffre d'affaire de l'entreprise, comme dans le RGPD ce qui n'est pas le cas dans l'avant-projet.

4. **Consentement :** Il serait important de préciser l'obligation **pour les tiers collectant et traitant des données** à caractère personnel de recueillir le consentement des personnes concernées, préalablement à la collecte. Cela s'applique aussi aux cookies. **Une présomption de non-consentement** pour le transfert de données aux tiers devrait exister. En outre, le consentement de la personne concernée est recueilli pour une finalité spécifique. Avant chaque nouveau traitement effectué pour une nouvelle finalité, le consentement de la personne concernée devrait de nouveau être recueilli. Ce consentement devra être libre, spécifique, éclairé, univoque, comme le prévoit le RGPD.

5. **Le droit à la portabilité des données** : Il a été supprimé de l'avant-projet. Ce droit autorise les personnes concernées à obtenir et à réutiliser leurs données personnelles à des fins qui leur sont propres dans des services différents. Selon le RGPD, les organisations doivent fournir les données dans un format structuré, couramment utilisé, lisible par machine. Les organisations doivent répondre aux requêtes des personnes concernées dans un délai d'un mois. Le droit à la portabilité des données a pour objectif de rééquilibrer les relations entre les fournisseurs de services et les consommateurs. Il s'agit donc d'un droit important, qui devrait figurer dans la loi suisse sur la protection des données.

6. **Profilage et décision automatisée :** Selon le RGPD, les personnes concernées ont le droit de ne pas être soumises à des décisions automatisées qui produisent des effets légaux ou affectent considérablement la personne. Un **droit d'explication** devrait être expressément reconnu à toute personne recevant une décision prise sur la base d'un processus automatisé. Ce droit d'explication est fondamental pour éviter les discriminations (biais encodés) et de donner à la personne la possibilité de comprendre le fonctionnement de l'algorithme à l'origine de la décision.

7. **Mineurs :** Les mineurs méritent une protection spécifique en ce qui concerne les données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement de données à caractère personnel. Le RGPD indique en outre que les décisions automatisées ne doivent pas concerner les enfants. L'article 8 du Règlement général à la protection des données relatif aux enfants devrait être repris dans son intégralité dans le projet de loi suisse sur la protection des données.

**Nous proposons en outre les améliorations suivantes :**

8. **Certification :** Le RGPD impose aux organisations une obligation de sécurisation des données. Cette obligation de sécurisation des données est fondamentale du fait notamment de l'entrée en vigueur de la directive sur les paiements (PSD2) en janvier 2016 (avec une période de transition de 2 ans), qui oblige les établissements financiers à mettre les données de leurs clients à disposition des tiers, entrainant une désintermédiation du marché des paiements et un risque de faille de sécurité accru. Nous sommes favorables à un processus de certification **obligatoire** en matière de sécurité de données et **non pas seulement facultatif.** Cette certification viendra renforcer la confiance des consommateurs et des investisseurs, ce qui devrait également être profitable aux entreprises suisses.

9. **Propriété des données :** Nous proposons d'introduire dans le projet de loi que la personne concernée (data subject) reste la **propriétaire** de ses données et en **garde le contrôle de ses données** durant tout le traitement. Ce principe découle du fait que le droit à la protection des données est un droit fondamental qui est garanti par la Constitution Suisse (Art. 13) et par la Charte des droits fondamentaux (Art. 8).

10. **Norme ISO /Audit** : Nous encourageons par ailleurs la Suisse à développer avec d'autre Etats une norme ISO relative à la **transparence des algorithmes**. Les entreprises pourraient tirer un avantage comparatif de leur certification ISO en matière de transparence des algorithmes. Ensuite, un processus de notation des algorithmes serait également

souhaitable, afin d'évaluer la qualité de la programmation et le degré de transparence de l'algorithme et éviter les black boxes. A titre d'exemple, nous pouvons citer les véhicules autonomes. Des constructeurs automobiles vont en effet acheter ou développer des systèmes de pilotage automatique, élaborés sur la base d'algorithmes. Ces systèmes de pilotage vont avoir un impact sur la vie humaine. Une certification spécifique augmenterait la qualité des algorithmes sur le marché, renforcerait la confiance des acteurs et faciliterait l'acceptation sociale des produits utilisant des algorithmes. En cas d'accident, la victime pourrait se retourner contre le constructeur en apportant la preuve que l'algorithme utilisé était de mauvaise qualité.

11. **Audit en matière de protection des données.** Un audit spécifique à la protection des données serait judicieux pour accompagner les entreprises de grande taille dans leur mise en conformité. Les recommandations des audits seraient bénéfiques à l'ensemble des acteurs car elles renforceraient la qualité de la gouvernance des données dans les organisations ainsi que la réputation des entreprises en matière de protection des données. Elle renforcerait également la confiance des consommateurs dans les produits et services mis à disposition.

Conclusion

La réforme en matière de protection des données constitue une formidable opportunité tant pour les personnes privées dont les droits sont renforcés que pour les entreprises suisses. En effet, cette réforme peut venir renforcer la confiance de l'ensemble des acteurs (clients, fournisseurs et investisseurs) et créer un avantage concurrentiel pour les entreprises, source de nouvelles parts de marchés. Plus qu'un simple enjeu de conformité, il s'agit d'un véritable enjeu de confiance,[1] à l'aube d'une nouvelle révolution digitale pleine de promesses.[2]

[1] Zamboni, Alessandro, Billois, Gerome, Brun Raphael, Dufau-Sansot, Youri, La vie privée à l'ère du numérique, au-delà de la conformité, un enjeu de confiance, 24 janvier 2017, URL : https://www.wavestone.com/fr/insight/vie-privee-numerique-conformite-confiance/.

[2] Purdy, Mark, Daugherty, Paul, Why Artificial Intelligence is the future of Growth?, 2016, URL : https://www.accenture.com/lv-en/_acnmedia/PDF-33/Accenture-Why-AI-is-the-Future-of-Growth.pdf.