Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

GUTACHTEN

ZUM DATENSCHUTZRECHT

IN ARGENTINIEN, JAPAN, NEUSEELAND, SINGAPUR, SÜDKOREA, UND DEN USA

Endversion

Avis 15-196

Lausanne, 3 août 2016
LHU / AA / JC / KTD / gz

origny • CH-1015 Lausanne
él. +41 (0)21 692 49 11
ax +41 (0)21 692 49 49
ww.isdc.ch

INHALTSVERZEICHNIS

I. SACHVERHALT

L'Office fédéral de la justice est en train d'élaborer un projet de révision de la loi sur la protection des données. Le projet doit notamment contenir, selon le mandat du Conseil fédéral, les mesures qui permettront à la Suisse de se conformer au droit européen, actuel et futur (soit le paquet de réformes de l'UE, la Convention 108 modernisée et les recommandations reçues dans le cadre de l'évaluation Schengen 2014). Or, il ressort de plus en plus souvent des débats qui entourent la révision de la loi que l'Europe n'est pas tout, et que les gros interlocuteurs économiques de la Suisse sont désormais, ou seront, des pays extra-européens.

L'idée serait de confier un mandat à l'ISDC afin de faire le point sur la législation en matière de protection des données de certains pays non-européens, et notamment de savoir si on y trouve des dispositions analogues à celles que nous envisageons d'introduire dans notre projet s'y trouvent ou si ces pays ont une approche différente.

II. FRAGESTELLUNG UND METHODE

Gemäss dem Bundesamt für Justiz interessieren folgende Fragen:

Sur le fond, les questions qui nous intéressent concernent en particulier les pouvoirs, l'organisation et le fonctionnement des autorités de contrôle, les mesures prises ou envisagées pour répondre aux défis du big data et du profiling, les droits des particuliers notamment en matière de transparence et leurs possibilités d'agir (notamment l'existence de procédures de médiation), les devoirs des responsables du traitement (études d'impact, devoir de documentation notamment) ou encore les moyens de promouvoir la privacy by design et la privacy by default etc. (cf. pour le surplus le Rapport du groupe d'accompagnement de la révision de la LPD du 29 octobre 2014, publié sur le site Internet de l'OFJ, en allemand et en français).

Pour ce qui est des pays, nous avions pensé aux USA (vu notamment les événements récents en lien avec le Safe Harbor), à la Nouvelle-Zélande (qui est en train de moderniser sa législation), à un pays d'Amérique du Sud (l'Argentine par exemple), ainsi qu'à l'Asie (par exemple la Corée du Sud).

S'agissant des USA, l'ISDC avait déjà fait un point de la situation pour l'OFJ en 2010 ère, dans un avis de droit établi lors de l'évaluation de la LPD (avis [09-207]). Il s'agirait là d'actualiser et de compléter ce qui avait été fait à l'époque.

Auf dieser Grundlage wurde in Absprache mit dem Bundesamt für Justiz entschieden, das Recht von Argentinien, Japan, Neuseeland, Singapur, Südkorea auf folgende Fragen zu untersuchen:

1. Welche Befugnisse hat die Aufsichtsbehörde ? Wie wird ihre Unabhängigkeit gewährleistet (Organisation, Finanzierung, usw.)? Bestehen „Best Practices" / „Gute Beispiele"?
2. Welche Rechte stehen den Betroffenen zu (Rechtsweg, Mediation)
3. Welche Pflichten haben die für die Datenbearbeitung verantwortlichen Personen? Bestehen Dokumentationspflichten und Pflichten zur Vornahme eines „Privacy Impact Assessment"?
4. Welche Massnahmen werden ergriffen, um mit technischen Herausforderungen wie „Big Data", „Profiling" oder dem „Internet der Dinge" umzugehen?
5. Wie werden „Privacy by Design" und „Privacy by Default" gefördert?
6. Bestehen Vorschriften zur Datenportierung (Eigentum der Daten)?

Die Länderberichte fassen in erster Linie die jeweiligen Gesetzgebungen in Bezug auf die verschiedenen Fragen zusammen – weitergehende Informationen wurde angesichts fehlender

Verfügbarkeit entsprechender Lehre und Rechtsprechung eher selten berücksichtigt. Dies beruht auch darauf, dass die meisten der besprochenen Gesetze sehr neu sind. Zudem wurden die Länderberichte aufgrund des Personalbestands des SIR durchwegs von Juristinnen und Juristen verfasst, welche zwar in der Regel gewisse Erfahrungen mit den betroffenen Rechtsordnungen haben, aber in den betreffenden Staaten nicht studiert haben und dort entsprechend auch nicht zugelassen sind. Entsprechend konnte nicht überall der Kontext der Gesetzgebung umfassend berücksichtigt werden. Angesichts des Zwecks des Gutachtens vermittelt dieses aber doch einen nützlichen Einblick in die betreffenden Rechtsordnungen.

Bezüglich der USA enthält der Länderbericht lediglich eine kurze Übersicht über die neusten Entwicklungen. Entsprechend ist der Länderbericht nicht wie die anderen gegliedert und folgt deshalb am Schluss.

III. LÄNDERBERICHTE

A. ARGENTINIEN

Introduction

1. L'autorité de contrôle

L'autorité responsable du contrôle de la protection de données en Argentina est la Direction nationale de protection de données personnelles (*Dirección Nacional de Protección de Datos Personales* – « DNPDP »).

1.1. Fonctions et pouvoirs

La DNPDP est chargée de veiller à l'application de la législation sur la protection de données. En vertu de l'art. 29 de la Loi 25.326[1], elle remplit, notamment, les fonctions suivantes :

a) assiste et conseille les personnes qui en ont besoin, sur le champ d'application de la protection des données personnelles, ainsi que sur les moyens juridiques disponibles pour défendre leurs droits;
b) dicte les normes et les règlements à respecter dans le cadre de la loi 25.326;
c) réalise un recensement des fichiers, dossiers et bases de données soumis à la loi 25.326 et maintient un registre permanent de ceux-ci;
d) surveille le respect des règles sur l'intégrité et la sécurité des données par les responsables des archives, registres et bases de données contenant des données personnelles. Pour ce faire, la DNPDP peut demander une autorisation judiciaire afin d'accéder aux locaux, équipements et programmes de traitement de données pour vérifier les infractions à la loi 25.326;
e) sollicite des informations aux entités publiques et privées - notamment des documents, programmes ou autres éléments - relatifs au traitement des données personnelles. Dans ces cas, la DNPDP doit garantir la sécurité et la confidentialité des informations fournies;
f) impose des sanctions administratives en cas de violation de la législation sur la protection de données;
g) se constitue plaignante dans les actions pénales sanctionnant la violation de la législation sur la protection de données;
h) surveille le respect des exigences et garanties nécessaires par les bases de données privées destinées à fournir des renseignements, afin d'être inscrits dans la registre crée par la loi 25.326.

L'art. 29 du Décret 1558/2001[2] dispose que la DNPDP établira des règles administratives et de procédure par rapport au **registre des bases de données personnelles** (« le Registre »), ainsi que des informations techniques concernant le traitement et les conditions de sécurité des fichiers, dossiers et bases de données publiques et privées contenant des données personnelles. En autre, le Décret 1558/2001 prévoit que la DNPDP traitera les **plaintes et réclamations déposées** aux termes de la loi

---

1 Ley 25.326, Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Sancionada: Octubre 4 de 2000, disponible sous http://www.jus.gob.ar/media/33481/ley_25326.pdf (11.01.16).

2 Decreto 1558/2001, Proteccion de los datos personales, disponible sous http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf (11.01.16).

25.326, percevra les taxes d'inscription dans le Registre et organisera et assurera le bon fonctionnement de celui-ci (art. 21 de la loi 25.326).

Dans un autre domaine, la DNPDP est chargée **d'approuver les codes de conduite** adoptés par les entités représentatives des usagers ou responsables de bases de données (art. 30 de la Loi 25.326). Ceci se fait en tenant compte de la représentativité des entités en question pour l'adaptation de ces codes, de la législation sur la protection de données personnelles, et de l'effectivité des codes proposés par rapport aux opérateurs dans le secteur. En particulier en ce qui concerne les pénalités ou les mécanismes adéquats pour assurer la protection des données personnelles.

L'indépendance de la DNPDP est garantie par l'art. 29.2 de la loi 25.326 selon lequel, la DNPDP bénéficie **d'une autonomie fonctionnelle** et agit en tant qu'autorité décentralisée dans l'orbite du Ministère de la justice et des droits humains[3]. En vertu de l'art. 29 du Décret 1558/2001, le budget de la DNPDP est constitué par les taxes perçues en raison de services rendus, par les amendes imposées par le non-respect des lois sur la protection des données et, principalement, par le financement prévu dans la loi sur le budget de l'administration nationale.

1.2. Constitution

Les organes de la DNPDP sont le **Directeur**, le **Conseil consultatif,** le **Registre et le personnel**.

La DNPDP est dirigée et administrée par un **Directeur**, qui est nommé pour une période de 4 ans par le gouvernement avec l'accord du Senat. Le Directeur doit se consacrer exclusivement à sa fonction ; il est soumis aux règles sur l'incompatibilité des fonctions qui s'appliquent aux fonctionnaires de l'État. En cas de mauvaise gestion, le Directeur peut être démis de ses fonctions par le gouvernement.

L'art. 29 du Décret 1558/2001 prévoit la création d'un **Conseil consultatif** qui conseille « *pro bono* » le Directeur de la DNPDP. La constitution de ce Conseil est la suivante :

a) un représentant du Ministère de la justice;
b) un magistrat du parquet (*Ministerio público fiscal*) spécialisé en la matière;
c) un représentant des responsables des fichiers privés destinés à fournir des informations (nommé par la Chambre qui réunit les institutions nationales d'information sur le crédit);
d) un représentant de la Fédération des entités entrepreneuriales d'informations commerciales de l'Argentina (*Federacion de entidades empresarias de informaciones comerciales de la República Argentina*);
e) un représentant de la Banque centrale argentine;
f) un représentant des entreprises tenant des archives, registres ou bases de données pour la publicité;
g) un représentant du Conseil fédéral de la consommation;
h) un représentant de l'IRAM (Institut argentin des normes) spécialisé dans le domaine de la sécurité informatique;
i) un représentant de la superintendance des assurances;
j) un représentant de la Commission bicamérale du Congrès chargé du contrôle des organes et des activités relatifs à la sécurité intérieure et aux renseignements.

---

[3] Art. 29.2 de la loi 25.326 : « 2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación ».

L'art. 21 de la loi 25.326 prévoit la création d'un **Registre** (*Registro de archivos de datos*) auprès de la DNPDP. Le registre est le moyen d'identification et de contrôle des bases de données personnelles ; il est sous la responsabilité de La DNPDP. Tout fichier, archive et base de données public et privé destiné à fournir des renseignements (voir cf. 3) doit être inscrit auprès du Registre. L'inscription est une condition essentielle pour la légalité des bases de données contenant des informations personnelles. Lors de l'inscription dans le Registre, la DNPDP n'exige pas la divulgation du contenu des bases de données. Les modalités d'inscription sont peu formalistes ; celle-ci peut également être effectuée en ligne[4]. La dite inscription doit contenir au moins les informations suivantes :

a) nom et adresse de la personne responsable ;
b) la nature et l'objet de la base ;
c) la nature des données personnelles contenues dans chaque fichier ;
d) la méthode de collecte et de mise à jour des données ;
e) la destination des données et les personnes physiques ou juridiques auxquelles les données peuvent être transmises ;
f) la méthode d'interconnexion (*interrelación*) des informations enregistrées ;
g) les moyens utilisés pour assurer la sécurité des données dans la base, en détaillant les personnes ayant accès au traitement de l'information ;
h) la durée de conservation des données stockées ;
i) la forme et les conditions dans lesquelles les personnes peuvent accéder aux données et les procédures à effectuer pour corriger ou mettre à jour les données.

L'alinéa 3 de l'art. 21 de la loi 25.326 dispose également qu'aucun utilisateur ne peut avoir en sa possession des données personnelles autres que celles qui sont déclarées dans le Registre.

L'art. 29 du Décret 1558/2001 prévoit que la DNPDP soit doté de **personnel administratif** hiérarchiquement constitué et désigné par le Ministère de la justice. Celui-ci a un devoir de confidentialité concernant les informations dont il a eu connaissance pendant l'accomplissement de sa fonction.

2. Les droits des particuliers

2.1. Le droit d'accès, de rectification, d'actualisation et d'effacement de données

Le droit d'accès :
En vertu de l'art. 14 de la loi 25.326, les personnes concernées ont le droit de solliciter et d'obtenir de l'information sur leurs données personnelles stockées dans des bases de données destinées à fournir des renseignements, ceci que les bases de données soient publiques ou privées. Lorsqu'une demande est déposée, les responsables des bases de données doivent fournir les renseignements requis par les personnes concernées par leurs données ; ceci dans un délai de dix jours. Si le délai échoit sans obtenir les renseignements, les intéressés pourront agir par la voie d'un recours de *habeas data* (cf. 2.2).

Le droit de rectification, actualisation et effacement de données :
Selon l'art. 16 de la loi 25.326[5], les personnes physiques ont également le droit de demander la rectification, l'actualisation et/ou l'effacement des données qui les concernent. Le responsable de la

---

4 M. D'Auro & I. de Achaval, Data protection in Argentina: Overview, 2014, disponible sous http://global.practicallaw.com/3-586-5566 (12.01.16).

5 Art. 16 loi 25.326 : « (Derecho de rectificación, actualización o supresión).

base de données a un délai de cinq jours, à compter du dépôt de la demande, pour donner une suite favorable ou non à la demande (art. 14.2 loi 25.326). Ce dernier peut refuser une demande de rectification, d'accès ou d'effacement de données personnelles lorsque cela est nécessaire pour la protection de l'État, l'ordre public ou la sécurité publique, ou les intérêts des tiers (art. 17, loi 25.326). La rectification, l'actualisation et/ou l'effacement des données personnelles inexactes ou incomplètes figurant dans les registres publics ou privés n'entraine aucun coût pour l'intéressé (art. 19 de la loi 25.326).

2.2. La protection judiciaire : le recours de « *habeas data* »

Le recours en « *habeas data* » ouvre la voie judiciaire aux des personnes concernées par la protection de leurs données personnelles.

En Argentine, l'art. 19 de la Constitution et l'art. 1770 bis du Code civil[6] consacrent le droit à la protection de la vie privée. S'agissant du cas spécifique des bases de données contenant des

---

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.
3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.
4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.
5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.
7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos ».

[6] Constitution argentine, art. 19: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. [...]" ; Code civil argentin, art. 1770: "Protección de la vida privada. El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias. Además, a pedido del agraviado, puede ordenarse la publicación de la sentencia en un diario o periódico del lugar, si esta medida es procedente para una adecuada reparación", disponible sous http://www.infojus.gob.ar/docs-f/codigo/Codigo_Civil_y_Comercial_de_la_Nacion.pdf (15.01.16). La version antérieure de cette disposition (art. 1.071 bis du Code civil argentin, qui était en vigueur jusqu'au 31.07.15), conditionnait l'application de cet article au fait que les faits reprochés ne constituent pas un délit pénalement réprimé: "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado,

informations personnelles, l'article 43 de la Constitution institue, à l'instar du recours en « *habeas corpus* »[7], le recours en « *habeas data* »[8].

Un recours en *habeas data* peut être interposé par toute personne qui souhaite **obtenir des informations sur ses données personnelles** enregistrées dans une base de données et, le cas échéant, demander leur rectification, leur suppression, leur maintien confidentiel, leur mise à jour si elles sont inexactes, obsolètes ou fausses. Le recours en *habeas data* est ouvert en matière de bases de données publiques et privées (art. 33 de la loi 25.326). Si les données sont stockées dans des bases de données privées, celles-ci doivent être conçues dans le but de fournir des renseignements à des tiers (art. 14.1 loi 25.326[9]).

Le recours en *habeas data* s'exerce une fois épuisées les voies décrites sous cf. 2.1., sans que la personne lésée ait obtenu satisfaction (art. 38.2 de la loi 25.326). La **légitimation active** (art. 34 de la loi 25.326) en matière de recours en *habeas data* appartient à la personne lésée, son représentant légal, ses tuteurs ou ses curateurs et à ses successeurs en ligne directe ou collatérale jusqu'au deuxième degré. Quant à la **légitimation passive**, elle appartient aux responsables et aux utilisateurs des bases de données (art. 35 de la loi 25.326).

S'agissant de la forme, le recours en *habeas data* doit être interposé par **écrit** en mentionnant précisément le nom et la localisation de la base de données et, le cas échéant, le nom du responsable ou de l'utilisateur concerné. Si la base de données est publique, il faudra identifier l'entité responsable de celle-ci. Sur le fond, le recourant doit alléguer les faits pour lesquels il estime que les informations le concernant sont discriminatoires, fausses ou inexactes.

Suite à l'introduction du recours, le juge pourra ordonner des mesures provisoires, en particulier le **blocage temporaire des dossiers manifestement discriminatoires, faux ou inexacts** (art. 38 de la loi 25.326). Sur le fond, il jugera après avoir entendu le responsable de la base de données se prononcer sur les allégations du recourant. Si le recours est admis, le juge peut ordonner la **suppression, la rectification ou la mise à jour** des données personnelles ainsi que la confidentialité des informations concernées ; ceci en fixant un délai pour l'exécution de sa décision. Enfin, la sentence est communiquée à la DNPDP (art. 43 de la loi 25.326).

---

ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación", disponible sous http://www.infoleg.gov.ar/infolegInternet/anexos/105000-109999/109481/texactley-340_libroII_S2_tituloVIII.htm (14.01.16).

7 Le recours « Habeas corpus » permet de présenter rapidement devant un juge un recours afin que ceui-ci statue sur la validité d'une arrestation. L'art. 3 de la loi : dispose : « Corresponderá el procedimiento de hábeas corpus cuando se denuncie un acto u omisión de autoridad pública que implique: 1° Limitación o amenaza actual de la libertad ambulatoria sin orden escrita de autoridad competente ».

8 M. Mongiardino, Análisis de la figura del habeas data: su situación en Argentina, disponible sous http://www.aadat.org/analisis_figura43.htm (14.01.16).

9 Art. 14 loi 25.326 : « (Derecho de acceso). 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales".

La législation sur la protection de données ne fait aucune mention sur une éventuelle procédure de **médiation** en matière de bases de données personnelles. L'art. 5 e) de la Loi 26.589 sur la médiation et la conciliation obligatoires[10], exclut expressément l'obligation de soumettre un conflit à la médiation lorsque celui-ci concerne un recours en *habeas data*[11]. En revanche, au niveau des provinces cela n'est pas forcément le cas. En effet, la Loi 8858 de la Province de Córdoba[12] sur la médiation volontaire ne prévoit pas l'exclusion des conflits concernant le *habeas data*.

3. Les devoirs des responsables de traitement

Les principales obligations imposées aux responsables du traitement de données personnelles sont l'inscription des bases de données au Registre, de veiller à la sécurité des données stockées, la confidentialité et la fourniture des documents et renseignements sollicités par la DNPDP. Parmi d'autres obligations se trouvent notamment celles d'obtenir le consentement des personnes concernées par les données stockées, de limiter de l'objet de la collecte, de veiller à l'exactitude et la bonne qualité des données collectées. Ces obligations sont traitées ci-dessous au point 4.

Inscription dans le registre :
A teneur des articles 3 et 21 de la loi 25.326, toute base de données – publique et privée destinée à « fournir des renseignements », doit être inscrite au Registre. L'art. 24 du même dispositif abonde en disposant que les personnes physiques qui constituent une base de données qui n'est pas destinée à « utilisation exclusivement personnelle », doivent également les inscrire au Registre. Une base de données est définie comme « fournissant des renseignements » lorsque celle-ci permet à des tiers d'obtenir des informations sur une personne[13]. La Loi 25.326 ne mentionne pas que la base doit servir exclusivement à la fourniture de renseignements. Quant au concept « d'utilisation exclusivement personnelle », celui-ci est interprété dans le sens d'une utilisation exclusive de la base de données par le responsable, sans que l'information soit accessible à des tiers.

Sécurité :
Selon l'art. 9 de la Loi 25.326, les responsables de bases de données contenant des informations personnelles doivent adopter une série de mesures techniques et d'organisation, ceci afin de garantir la sécurité et la confidentialité des données. Il s'agit notamment d'éviter la détérioration ou la perte des données et de prévenir la consultation ou le traitement par des personnes non-autorisées. Il est aussi question d'éviter et de détecter des détournements (volontaires ou non) de l'information stockée, tant en raison d'une intervention humaine que technique. Il est formellement interdit de

---

10 Ley 26.589, Mediación y conciliación, Establécese con carácter obligatorio la mediación previa a procesos judiciales, Mayo 3 de 2010, disponible sous http://infoleg.mecon.gov.ar/infolegInternet/anexos/165000-169999/166999/norma.htm (14.01.2016), art. 5 : « Controversias excluidas del procedimiento de mediación prejudicial obligatoria. El procedimiento de mediación prejudicial obligatoria no será aplicable en los siguientes casos [...] e) Amparos, hábeas corpus, hábeas data e interdictos ».

11 C. Corzo, Habeas data colectivo, 2012, disponible sous http://p3.usal.edu.ar/index.php/institutas/article/view/1992/2427 (14.01.16); . L. Giannini, Experiencia argentina en la mediación obligatoria, 2014, disponible sous http://www.academia.edu/6001736/Experiencia_de_la_mediaci%C3%B3n_en_Argentina_LL_5-2-2014_ (15.01.16).

12 Ley Nº 8858, Mediación, B.O. 14.07.00, Fecha de sanción: 28.06.00, disponible sous http://web2.cba.gov.ar/web/leyes.nsf/85a69a561f9ea43d03257234006a8594/bd4221bfcfac6ec20325723400648342 (20.01.16)..

13 Protection de données personnelles, Présidence de la Nation et Ministère de la justice, disponible sous http://www.jus.gob.ar/datos-personales/cumpli-con-la-ley/¿cuales-son-tus-obligaciones.aspx (11.01.16).

stocker des données personnelles dans des bases de données qui ne remplissent pas les garanties de sécurité. Il n'existe pas une obligation des responsables de bases de données personnelles d'informer la DNPDP sur des failles de sécurité détectées, mais ceux-ci doivent mettre en œuvre les instructions du Manuel sur la protection de la sécurité des données prévues dans la Disposition 11/2006 de la DNPDP (cf. également, ci-dessous, 5.)[14]. Entre les obligations imposées aux responsables par cette dernière se trouve celle de tenir un dossier de sécurité qui précise, entre autres, les procédures et les mesures de sécurité mises en œuvre. Le dossier de sécurité doit être tenu à jour en cas de changements dans le système d'information. Le dossier[15] doit contenir notamment :

1. les tâches et responsabilités du personnel en charge de la base de données ;
2. une description des fichiers contenant des données personnelles et des informations sur les applications qui les traitent ;
3. une description des procédés de contrôle des données, des programmes et des procédures de saisie de données à prendre, ceci afin de corriger des erreurs détectées. Tous les programmes de saisie de données, quel que soit le mode de traitement (batch, interactif, etc.) doivent inclure dans leur design (voir cf. 4), des moyens de contrôle qui minimisent la possibilité d'intégrer au système des données illogiques ou erronées ;
4. le registre d'incidents de sécurité détectés ainsi que les notifications, les gestions et les mesures adoptées à chaque type d'incidents ;
5. les procédures mises en place pour sauvegarder et récupérer des données ;
6. la relation actualisée entre les systèmes d'information et les usagers des données ;
7. les procédures d'identification et d'authentification des utilisateurs autorisés à utiliser le système.

Confidentialité :
Le responsable et les personnes intervenant à n'importe quel moment dans le traitement de données sont soumis au secret professionnel (art. 10 de la loi 25.326). Cette obligation subsiste au-delà de la fin de l'autorisation d'accès à la base de données.

Devoir de fournir des documents et renseignements :
L'art. 31 de l'Annexe I du Décret 1558/01, tel que modifié par le Décret 1160/2010 du 11.8.10[16], dispose à l'alinéa 3, que la DNPDP peut réaliser des enquêtes et contrôles, ainsi que demander, aux responsables ou aux utilisateurs de bases de données personnelles, la fourniture d'informations, des documents, des programmes, des antécédents et d'autres éléments relatifs au traitement des données stockées. La DNPDP peut aussi exiger que les responsables des bases de données préparent des rapports portant sur leur base de données et le traitement de données qu'ils y effectuent.

Sanctions :
En cas de violation par les responsables des obligations concernant leurs bases de données, la loi prévoit des sanctions administratives, disciplinaires et civiles, incluant la clôture de leurs bases de

---

14 Disposición 11/2006, Apruébanse las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados", Bs. As., 19/9/2006, disponible sous http://www.jus.gob.ar/media/33445/disp_2006_11.pdf (15.01.16).

15 Un modèle de dossier de sécurité se trouve dans la Disposition 9/08, disponible sous http://www.jus.gob.ar/media/33466/disp_2008_09.pdf (15.01.16).

16 Decreto 1160/2010, Protección de los datos personales, Modifícase el Anexo I del Decreto Nº 1558/01, Bs. As., 11/8/2010, disponible sous http://www.jus.gob.ar/media/2681318/decreto_1160_2010.pdf (15.01.16).

données (art. 31 de la loi 25.326[17]). L'art. 32 de la même loi[18] a modifié l'art. 117 du code pénal en prévoyant des sanctions pénales.

4. Mesures prises concernant Big Data et Profiling et l'internet des objets

4.1. Big Data

La première question qui se pose par rapport à la collecte de Big Data est celle de savoir si une telle activité est soumise à la Loi 25.326 et aux dispositions règlementaires sur la protection des données personnelles. La réponse à cette question semble être affirmative. En effet, si les données cumulées dans le cadre de la Big Data peuvent être considérés comme des « données personnelles » et s'il s'agit d'archives, registres, bases de données ou d'autres moyens techniques de traitement de données, l'activité tombera sous le coup de la Loi 25.326[19] (et de l'art. 43 de la Constitution argentine[20]). Ainsi, la **législation sur la protection des données s'appliquera à la collecte de Big Data** lorsque de l'ensemble des donnés collectées, il ressort que celles-ci désignent une personne en particulier (et ceci même lorsque l'une des informations faisant partie de la Big Data ne fait pas référence à une personne

---

17 Loi 25.326, Art. 31: « (Sanciones administrativas). 1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.
2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso ».

18 Loi 25.326, Art. 32: « (Sanciones penales). 1. Incorpórase como artículo 117 bis del Código Penal, el siguiente: "1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".
2. Incorpórase como artículo 157 bis del Código Penal el siguiente:
"Será reprimido con la pena de prisión de un mes a dos años el que:
1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años" ».

19 L. Gandolla, Conflictos entre el Big Data y la Ley de Protección de Datos Personales, 13.11.15, disponible sous http://www.infojus.gob.ar/luciano-gandolla-conflictos-entre-big-data-ley-proteccion-datos-personales-dacf150830-2015-11-13/123456789-0abc-defg0380-51fcanirtcod (11.1.16).

20 Constitution argentine, art. 43 « [...] Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística », disponible sous http://www.senado.gov.ar/delnteres (12.01.15).

spécifique)[21]. En revanche, sont exclus de l'application de la législation sur la protection de donnés, les données Big Data qui ne peuvent pas être associés à une personne en particulier – comme, par exemple des données statistiques ou techniques.

Dès lors que l'application de la législation sur la protection des donnés à la collecte de Big Data semble acquise. Cette dernière pose une **série de problèmes pratiques**, en raison de l'éventuelle collision entre cette activité et certains des principes qui régissent la protection de données personnelles. Parmi les domaines susceptibles de causer de telles collisions, se trouvent le principe du **consentement**[22], celui de la **limitation de l'objet de la collecte de données**, et encore ceux de l'obligation **d'exactitude**[23] et de la **qualité** des données.

En raison de ces collisions, la loi argentine sur la protection de données personnelles nécessitera probablement une **adaptation** afin de couvrir le phénomène du Big Data, car il s'agit d'un développement qui n'est pas encore réglé de manière satisfaisante. Un auteur souligne à cet égard:

> « La difficulté ne se concentre pas sur le fait d'obtenir de ceux qui collectent de Big Data se soumettent aux normes de protection des données personnelles, mais d'élaborer, avec la participation de la plus grande quantité possible d'acteurs, des lignes directrices pour cette nouvelle réalité, tout en respectant la vie privée personnes. »[24].

4.2. Profiling

L'art. 27 du Décret 1558/2001[25], contient une règle sur le **profilage dans le domaine de la publicité**. Selon cette disposition des données peuvent être collectées, traitées et transmises à des fins publicitaires sans le consentement de la personne, lorsque le but est celui de créer de profiles destinés à catégoriser des préférences et des comportements. Ceci est assorti d'une double condition, à savoir que les personnes concernées ne soient identifiés que par leur appartenance à un groupe générique, et que les données individuelles incluses soient seulement les strictement nécessaires. Les associations, chambres et collèges professionnels qui réalisent du profilage doivent adopter une réglementation prévoyant l'élimination ou le blocage des supports de données publicitaires lorsqu'un

---

21 L. Gandolla, op. cit.

22 L. Gandolla, op. cit.

23 L. Gandolla, op. cit.

24 L. Gandolla, op. cit. : « La dificultad no se centra en lograr que quienes realizan Big Data cumplan con las normas de protección de datos personales, sino en generar, con la participación de la mayor cantidad de actores posible, directrices aplicables a esta nueva realidad, respetuosas de la privacidad de las personas ».

25 Decreto 1558/2001, Art. 27 : « Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios. Las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DNPDP, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de Aplicación, implementarán, dentro de los noventa (90) días siguientes a la publicación de esta reglamentación, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros. En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información".

particulier le demande. Le retrait ou le blocage peut être total ou partiel et, à la demande de la personne concernée, ceux-ci peuvent s'appliquer un ou à plusieurs vecteurs de diffusion (tels que le courrier, le téléphone, le courriel, etc.).

Dans toute communication à des fins publicitaires faite par courrier, téléphone, courrier électronique, Internet ou autre moyen de transmission à distance, il faudra indiquer – expressément et en souligné – la possibilité pour le titulaire des données de **demander le retrait ou le blocage** mentionnés. A la demande de la personne concernée, on doit fournir le nom du responsable ou de l'utilisateur de la base de données ayant transmis l'information.

L'art. 20 de la loi 25.326[26], dispose que les **décisions judiciaires ou les actes administratifs** qui impliquent une évaluation ou une appréciation de comportement humains ne peuvent pas avoir comme seul fondement, le résultat d'un **traitement informatisé de données personnelles fournissant une définition du profil ou de la personnalité d'une personne**. Les actes contraires à ce qui précède sont nuls. Cette disposition s'inspire de l'art. 13 de la loi espagnole sur la protection de données[27]. Toutefois, contrairement à la loi espagnole, l'art. 20 de la loi 25.326 ne prévoit pas la possibilité de contester (*impugnar*) les données stockées dans des bases de données privées, ni d'exiger du responsable de la base de données en cause de lui fournir les critères d'évaluation et les programmes utilisés pour le traitement des données problématiques. Un auteur souligne que, malgré cette omission, en Argentina le droit de contestation peut exister même à l'encontre de bases de données privées[28]. En outre et malgré l'omission de la possibilité d'obtenir les critères d'évaluation et les programmes utilisés pour le traitement des données problématiques, cet auteur est d'avis que ceci serait possible, si on adoptait une interprétation extensive du droit d'accès[29].

4.3. Internet des objets

La législation argentine ne prévoit pas des normes spécifiques sur la protection de la vie privée par rapport aux objets, à savoir, notamment aux données compilés par les senseurs installés dans des

---

26 Loi 25.326, Art. 20 : « (Impugnación de valoraciones personales). 1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.
2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

27 Artículo 13. Impugnación de valoraciones. 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado": Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, TEXTO CONSOLIDADO, Última modificación: 5 de marzo de 2011, disponible sous http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf (12.01.15); L. Gandolla, op. cit.

28 L. Gandolla, op. cit.

29 L. Gandolla, op. cit.

maisons, véhicules ou appareils[30]. Des auteurs suggèrent qu'une actualisation législative sur l'Internet des objets peut s'avérer nécessaire[31].

5. Promotion de privacy by design / privacy by default

Selon le préambule de la Disposition 18/2015 de la DNPDP du 10/4/2015[32] une grande partie des traitements de données personnelles se réalise au moyen d'un logiciel (*software*) qui fonctionne de façon automatisée ou avec peu de surveillance humaine. Dès lors, afin de respecter la réglementation sur la protection de données personnelles, les applications doivent être conçues et développées de façon à respecter les droits des personnes concernées. A ce sujet la DNPDP a approuvé un **« Guide de bonnes pratiques dans le développement d'applications informatiques »** (« Le Guide »). Le Guide est un « document d'orientation » qui fixe des directives qui doivent être suivies pour respecter la protection de données personnelles lors de développements d'applications informatiques. Le préambule de la Disposition 18/2015 souligne encore que le respect du Guide sera une valeur ajoutée à la qualité des logiciels développés en Argentine.

Concrètement, le Guide **s'adresse aux développeurs d'applications** informatiques en leur soulignant qu'ils ont la responsabilité de veiller au respect de la vie privée des personnes, ceci à partir du moment où ils commencent le développement d'une application. Le développement doit tenir compte d'une politique d'utilisation des données qui soit claire et transparente et, qui permette aux personnes concernées de connaitre la façon dont le traitement de leurs données est réalisé.

Les notions de « *privacy par design* » et de « *privacy by default* » sont selon le Guide :

a. La « *privacy par design* » est définie comme une perspective selon laquelle à partir de l'origine même du design de l'application, le développeur tient compte de la protection de la vie privée. Autrement dit, la perspective de la protection des données personnelles ne doit pas, uniquement, être prise en compte au moment où l'application est mise à disposition du public, mais dès le développement de celle-ci. Le respect du droit à la protection des données doit se déployer tout au long de la vie de l'application.
b. La « *privacy par defaut* » correspond au fait que les protections introduites dans les applications doivent rester actives par défaut. Ceci obligera l'utilisateur à effectuer un acte volontaire pour les désactiver ou pour partager les informations stockées. La raison pour laquelle la protection par défaut est installée s'explique par le fait que les utilisateurs des applications, lorsqu'ils s'en servent, ne prennent pas toujours le temps ou ne savent pas comment configurer les options de protection des données.

Le Guide mentionne différents moyens de protection de la vie privée qu'on peut introduire dans les programmes :

1. **La dissociation** de données qui permet de cacher l'identité de la personne concernée afin d'éviter la mise en relation avec les données stockées ;

---

30 L. Pautasio, Internet de las Cosas en la industria del seguro, 28/12/2015, disponible sous http://www.revistaestrategas.com.ar/revista-592.html (22.03.16).

31 P. Segura, A un año de Rodríguez contra Google: ¿Estableció la CSJN un derecho al olvido digital en Argentina?, Id Infojus DACF150827, disponible sous ftp://ftp.justiciachaco.gov.ar/biblioteca/BIE/BIE_5_041215/Segura.pdf (22.06.16).

32 Disposición 18/2015 de la DNPDP, 10/4/2015, disponible sous http://www.jus.gob.ar/media/2854264/disp_2015_18.pdf (15.01.16).

2. **L'utilisation de pseudonymes** (*seudonimización*) permet la réalisation d'opérations sans utiliser le vrai nom de la personne concernée ;
3. **La sécurisation** qui empêche des intrus d'accéder aux bases de données sans autorisation ;
4. **Les métadonnées** permettent d'incorporer des étiquettes sur des archives contenant des données personnelles, en détaillant la source, le consentement obtenu, les utilisations permises et la politique de non-intromission dans la vie privée. En outre, elles permettent d'indiquer le temps pendant lequel les données peuvent conservées, ainsi que l'accord pour la transmission des données à des tiers ;
5. **L'encryptage** permet non seulement d'assurer le stockage sûr des données, mais aussi leur intégrité et la protection de l'accès.

La Disposition 11/2006 (cf. 3) impose aux responsables de bases de données **l'obligation d'utiliser des programmes de saisie de données** qui contiennent dans leur design des mécanismes de contrôle qui minimisent la possibilité de stocker des données illogiques ou erronées, et ceci quel que soit le mode de leur traitement (batch, interactif, etc.)[33].

La Disposition 18/2015 prescrit que le respect de la vie privée doit être pris en compte à tous les stades de « vie » du système, de l'application ou du dispositif, ceci en suivant les principes de la « *privacy by design* » et de la « *privacy by default* ». Le Disposition 18/2015 mentionne, également, la « ***Privacy-Enhancing Technologies*** **(PET)** »[34]. Cette procédure est définie comme un ensemble de mesures, d'instruments et d'applications qui protègent la vie privée dans le cadre de l'information stockée ; ceci par voie d'élimination ou de minimisation des données personnelles. Ainsi, on évite le traitement non-nécessaire ou non-désiré des données personnelles lors de l'utilisation du système d'information sans que celui-ci ne perd sa fonctionnalité.

6. Portabilité de données

Le droit argentin ne prévoit pas des dispositions spécifiques sur la récupération et portabilité des données. Toutefois, certains principes peuvent être tirés de normes qui règlent d'autres domaines. Ainsi, par rapport aux **consommateurs**, l'article 1113 du Code civil et commercial argentin[35], prévoit que lorsqu'une personne exerce son droit de résiliation d'un contrat de consommation, « les parties doivent se restituer réciproquement et de façon simultanée les prestations accomplies ». Une interprétation de cette disposition à la lumière du sujet de la protection de données pourrait mener à la conclusion que le consommateur peut demander la récupération de ses données qui se trouvent chez le fournisseur. Pour ce qui concerne les e-mails, il existe actuellement une **proposition de loi sur**

---

33 Disposición 11/2006, Annexe I, art. 3 : « [...] Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes ».

34 Disposition 18/2015 : « Privacy-Enhancing Technologies (PET) Se trata de un sistema de medidas, herramientas y aplicaciones que protegen la privacidad de la información mediante la eliminación o minimización de los datos personales. De ese modo se previene el procesamiento innecesario o indeseado de datos personales, sin la pérdida de la funcionalidad del sistema de información".

35 Codigo civil y Comercial de la Nación, Art. 1113 » : « Efectos del ejercicio del derecho de revocación. Si el derecho de revocar es ejercido en tiempo y forma por el consumidor, las partes quedan liberadas de sus obligaciones correspectivas y deben restituirse recíproca y simultáneamente las prestaciones que han cumplido », disponible sous http://www.notarfor.com.ar/codigo-civil-comercial-unificado/articulo-1113.php (22.03.16).

la protection du courrier électronique[36], qui assimile les courriels aux correspondances épistolaires dans tous les aspects, notamment dans la « création, la transmission et le stockage »[37]. L'art. 17 de la Constitution argentine ainsi que l'art. 6 de la Loi 20.216 sur la poste[38] consacrent le principe de l'inviolabilité de la correspondance épistolaire. Il est difficile à savoir si de ceci on peut tirer des conclusions par rapport à la récupération et portabilité de courriels.

---

36 Anteproyecto de ley de proteccion del correo electronico, Art 2º: "A los efectos legales, el correo electrónico se equipara a la correspondencia epistolar. La protección del correo electrónico abarca su creación, transmisión y almacenamiento", disponible sous http://delitosinformaticos.com/articulos/100046596135002.shtml (22.03.16).

37 L'art. 17 de la Constitution argentine ainsi que l'art. 6 de la Loi 20216 sur la poste [disponible sous http://legislatura.chaco.gov.ar/InformacionLegislativa/datos/textos/word/00007585.DOC (22.03.16)], consacrent le principe de l'inviolabilité de la correspondance épistolaire.

38 Ley Loi 20.216, disponible sous http://legislatura.chaco.gov.ar/InformacionLegislativa/datos/textos/word/00007585.DOC (22.03.16).

B. SÜDKOREA[39]

Einführung

Südkorea hat seit 2011 eine Gesetzgebung im Bereich des Datenschutzes, der Personal Information Protection Act (PIPA)[40], welche mindestens im asiatischen Vergleich als sehr progressiv angesehen wird[41]. Dazu bestehen Sondergesetze in Bezug auf IT Dienstleistungen[42] (inkl. Zu Lokalisierungsdienstleistungen[43]) sowie im Zusammenhang mit Finanzdienstleistungen[44] und Kreditinformationen[45], und für den öffentlichen Sektor sowie die Privatwirtschaft finden sich datenschutzrelevante Bestimmungen in weiteren Gesetzen.[46] In jüngster Zeit (2014) wurde die Bearbeitung der Einwohnerregistrationszahl (*Resident Registration Number*[47]) sowie die Weitergabe von Kundeninformationen innerhalb von Holdings eingeschränkt[48].

1. (Aufsichts-)behörden

Angesichts der Vielzahl von Gesetzen und aus historischen Gründen findet sich in Korea ein relativ komplexes Nebeneinander verschiedener Behörden mit teilweise überlappenden Zuständigkeiten. Dabei wird im Grundsatz zwischen **regulatorischen Fragen (*policy*)** und Behandlung individueller Beschwerde unterschieden. Für den ersten Bereich besteht eine eigene Kommission (***Personal Information Protection Commission***) unter dem Staatspräsidenten. Ein Beispiel von Angelegenheiten, mit denen sich die Kommission befasst, sind die als Entscheidung bezeichneten „Kommentare zu der von Google verwendeten *Privacy Policy*".[49] Im Bereich der Netzwerke hat die ***Korea Communications Commission*** ebenfalls wichtige Zuständigkeiten. Sie kann nicht nur Empfehlungen in Form von Richtlinien abgeben, sondern hat auch verschiedene Überwachungsbefugnisse (inkl. Zugangsbefugnisse und Sanktionsmöglichkeiten) gegenüber IT-Dienstleistungserbringern.[50]

---

39 Dieser Bericht beruht auf den am Schweizerischen Institut für Rechtsvergleichung sowie online vorwiegend in englischer Sprache verfügbaren Informationen.

40 Alle zitierten Gesetze sind in englischer Übersetzung auf der Website des Justizministeriums verfügbar: http://www.law.go.kr/eng/engMain.do.

41 S. dazu G. Greenleaf & Whon-il Park, Korea's new Act : Asia's toughest data privacy law, *Privacy Laws & Business International Report, Issue 117,* 1. – 6. Juni 2012, verfügbar auch unter SSRN (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2120983).

42 Seit 2001 der Act on Promotion of Information and Communication Network Utilization and Information Protection.

43 Act on the Protection, Use, Etc. of Location Information; Act on the Creation and Facilitation of Use of Smart Grids.

44 Act on Real Name Financial Transactions and Confidentiality.

45 Use and Protection of Credit Information Act.

46 So gemäss Graham Greenleaf, Asian Data Privacy Laws. Trade and Human Rights Perspectives, OUP 2014, S. 134, im öffentlichen Sektor der Act on Communication Secrets, der Telecommunications Business Act oder der Medical Services Act oder für die Privatwirtschaft der Act on Real Name Financial Transactions and Confidentiality, der Framework Act on Electronic Documents and Electronic Commerce oder der Electronic Signature Act.

47 Wohl vergleichbar mit der Sozialversicherungsnummer in der Schweiz.

48 Sky Yang, Korea tightens data protection rules, 23.02.2015, verfügbar unter http://www.iflr.com/Article/3429777/Korea-tightens-data-protection-rules.html.

49 Comments on Improvements of Privacy Policy of Google Inc., verfügbar in englischer Sprache unter http://www.pipc.go.kr/cmt/english/news/selectBoardArticle.do.

50 S. insbesondere Art. 64 des Act on Promotion of Information and Communication Network Utilization and Information Protection.

Für die Schlichtung **individueller** (aber auch kollektiver) **Beschwerden**, wurde ein eigenes Komitee, das ***Personal Information Dispute Mediation Comittee*** geschaffen. Dieses führt bei Divergenzen zwischen betroffenen Personen und datenbearbeitenden Institutionen eine „Mediation" durch und unterbreitet den Parteien einen Schlichtungsvorschlag, der negatorische, reparatorische und präventive Massnahmen enthalten kann (Art. 47 PIPA). In diesem Rahmen hat das Komitee gewisse Untersuchungsbefugnisse (Art. 45 PIPA: Einlieferung von Unterlagen, Anhörung von Zeugen), und kann auch bereits im Voraus eine Einigung vorschlagen (Art. 46 PIPA). Das Verfahren wird insbesondere ausgesetzt, wenn eine Partei ein Gerichtsverfahren anstrebt (Art. 48 PIPA). Beschwerden im IT-Bereich (*personal information infringements*) werden durch die ***Korea Internet & Security Agency*** (KISA) unter einer Hotline (118) entgegengenommen[51], wobei die KISA diesfalls auch Abklärungen vornimmt und bei grösseren Angelegenheiten die Vollzugsbehörden benachrichtigt.[52] Die KISA nimmt hier eine informelle Schlichtungsfunktion wahr, die oft vor dem formalisierten Verfahren das Mediation Committee stattfindet[53]. Die KISA hat zudem verschiedene Guidelines und Guides für den Privatsektor entwickelt.[54]

Schliesslich hat das **Innenministerium** (früher das Ministerium für Sicherheit und öffentliche Verwaltung) eine wichtige Rolle bei der Ausführung der Datenschutzgesetzgebung. Es führt insbesondere das Sekretariat der *Personal Information Protection Commission*, ernennt die Mitglieder des *Dispute Mediation Committee* und hat durchführende Funktionen. Diese betreffen z.B. die Ausarbeitung der Ausführungsverordnung zum PIPA sowie das Erstellen eines dreijährlichen Datenschutzplanes (*Data Protection Basic Plan*; Art. 9 PIPA), der von der Kommission genehmigt wird. Zudem werden allgemeine Richtlinien ausgearbeitet (Art. 12 PIPA), welche von den verschiedenen Ministerien und staatlichen Stellen für besondere Sektoren angepasst werden können.[55] Im Rahmen der Durchsetzung hat das Ministerium zudem eingehende Untersuchungsbefugnisse (Art. 63 PIPA) und kann die Suspendierung von Datenschutzverletzungen oder sogar der Datenbearbeitung anordnen (Art. 64 PIPA) sowie die Angelegenheit an die Untersuchungsbehörden überweisen. Das Ministerium kann schliesslich (nach Anhörung der Kommission) sogar die Identität von Verletzern der Datenschutzgebung, die Verletzung und die getroffenen Massnahmen veröffentlichen.[56]

2. Rechte der Betroffenen

Gemäss Art. 4 PIPA[57] haben die Betroffenen das **Recht auf Information** über die Bearbeitung von sie betreffenden Daten und diesbezüglich grundsätzlich das Recht auf Erteilen oder Nichterteilen ihrer Zustimmung. Sie sind ebenfalls berechtigt, die sie betreffende Information zu prüfen und **Aufhebung,**

---

51 So auch gemäss der Website der KISA : https://www.kisa.or.kr/eng/activities/internetsecurity.jsp#.

52 Greenleaf, Asian Data Privacy Laws, zit., S. 136.

53 Greenleaf, Asian Data Privacy Laws, zit., S. 149 f.

54 Greenleaf, Asian Data Privacy Laws, zit., S. 136.

55 S. zu all dem Greenleaf, Asian Data Privacy Laws, zit., S. 135.

56 Art. 66 PIPA.

57 A subject of information has the following rights in connection with the management of his/her personal information:
1. A right to receive information concerning the management of personal information;
2. A right to choose and decide whether he/she consents to the management of his/her personal information, the scope of consent, and related matters;
3. A right to verify whether personal information is managed and to request an inspection of personal information (including issuance of a certified copy; hereinafter the same shall apply);
4. A right to request the suspension, correction, deletion and destruction of personal information;
5. A right to receive relief from damage caused by the management of personal information according to prompt and fair procedures.

Korrektur oder Löschung der Information zu verlangen. Schliesslich sieht das Gesetz ein Recht auf **Schadenersatz** gemäss schnellem Verfahren vor.[58]

Hervorzuheben sind insbesondere die relativ strenge **Ausgestaltung der Zustimmung**, welche seitens der für die Datenbearbeitung verantwortlichen Personen weitgehende **Informationspflichten** vorsieht (s. unten, 3.)

Die Gesetzgebung zu **Netzwerk- und Kommunikationsdienstleistungen** sieht ebenfalls ein Recht des Betroffenen auf Zustimmung bzw. Widerruf der Zustimmung, Prüfung und Korrektur bzw. Löschung der persönlichen Information vor und verbietet die Bearbeitung von als falsch festgestellten Informationen (Art. 30 *Act on Promotion of Information and Communication Network Utilization and Information Protection,* im Folgenden «Netzwerk Gesetz»). Auch hier ist ein Recht auf Ersatz (*indemnification*) vorgesehen (Art. 32 Netzwerk Gesetz), mit der Möglichkeit auf pauschalierten Schadenersatz.

Am 29. April 2016 hat die *Korea Communications Commission* zudem Richtlinien über das «**Recht auf Vergessen**» herausgegeben.[59] Neben den insbesondere im Bereich des Netzwerk Gesetzes vorgesehen Massnahmen wie der vorläufige Rechtsschutzes bei Informationen, welche die Privatsphäre verletzt[60], sehen die Richtlinien vor, dass Nutzer den Administrator sowie Suchseitenbetreiber um das Entfernen von Informationen bitten, was dieser nur bei Bestehen einer gegenteiligen rechtlichen Pflicht oder eines öffentlichen Interesses verneinen soll. Vorgelegt werden muss der Beweis, dass die Informationen von der die Entfernung beantragenden Person erfolgte sowie eine Begründung für die Entfernung. Die Richtlinien sind zwar nicht rechtlich bindend, doch wird aufgrund des Drucks von den Konsumenten mit einer weitgehenden Berücksichtigung gerechnet.[61]

Bestimmungen zur Zustimmung bzw. deren Widerruf sowie zur Einsichtnahme und Korrektur finden sich auch in anderen Gesetzen.[62] Im Gesetz zur Lokalisierungsinformation ist schliesslich ein Recht auf Information über **allfällige Weitergabe der Information an Dritte** vorgesehen (Art. 24 Abs. 3).

3. Pflichten der für die Datenbearbeitung verantwortlichen Personen[63]

Im Rahmen der allgemeinen Pflicht zur Datenbearbeitung im gesetzlichen Rahmen (insbesondere im Rahmen der Zweckgebundenheit) ist zunächst die grundsätzliche **Pflicht zum Einholen der Zustimmung** der betroffenen Person zu erwähnen. Dabei muss die verantwortliche Person die Information, deren Bearbeitung (z.B. aufgrund eines bestehenden Vertrags) keine Zustimmung verlangt, von der Information, für deren Bearbeitung Zustimmung erforderlich ist, separat ausweisen (Art. 22 Abs. 2 PIPA). Ebenfalls muss eine besondere Zustimmung eingeholt werden, wenn die Information zur Vermarktung von Waren und Dienstleistungen verwendet wird (Art. 22 Abs. 3 PIPA).

---

58 S. dazu ausführlich Art. 35 ff. PIPA.

59 Guidelines on «the Right tob e Forgotten», s. Medienmitteilung der Korea Communications Commission vom 29.4.2016 (englische Version vom 16.06.2016), verfügbar unter http://eng.kcc.go.kr/user.do;jsessionid=DjQwlVclU4dGruqaJWXJmXKnCWQfLGtFjkOBduq1bWJuKg1oQe49btsKaMFZLQSM.hmpwas02_servlet_engine1?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=42538.

60 So gemäss Fn 2 der Pressemitteilung, welche sich wohl auf Art. 30 APICNU bezieht.

61 So gemäss dem ICT Legal Update 2016.05 der Anwaltskanzlei Yulchon, verfügbar unter www.yulchon.com.

62 Z.B. Art. 24 Law on Protection and Use of Location Information.

63 Im Rahmen des ersten Entwurfs beschränken sich die folgenden Ausführungen auf die in der allgemeinen Gesetzgebung vorgesehenen (PIPA) Pflichten.

Besonders zu bemerken ist diesbezüglich, dass das Erbringen von Dienstleistungen bzw. die Lieferung von Warren nicht verweigert werden darf, wenn die Zustimmung zu gewissen Bearbeitungen nicht erteilt wird (Art. 22 Abs. 4 PIPA). Um die Zustimmung zu erhalten, muss der Zweck der Datenbearbeitung, die Einzelheiten der persönlichen bearbeiteten Information, die Zeitdauer, während der die Information bearbeitet wird, und die Möglichkeit der Verweigerung der Zustimmung (sowie die entsprechenden Folgen) aufgezeigt werden (Art. 15 Abs. 2 PIPA).

Die für die Datenbearbeitung verantwortliche Person hat zudem die betroffene Person grundsätzlich[64] auf deren Aufforderung hin zu **informieren**, wenn sie persönliche Informationen bearbeitet, die sie von dritter Seite erhalten hat (Art. 20 PIPA).

Schliesslich muss die für die Bearbeitung verantwortliche Person die Information nach Ablauf des angegebenen Zeitraums bzw. nach Erfüllen des Zwecks **zerstören** (Art. 21 PIPA).

Neben diesen Verhaltenspflichten im Rahmen der Datenbearbeitung sieht der PIPA im Kapitel IV verschiedene **Sicherungsvorkehrungen** (*safeguards*) vor, welche die datenbearbeitende Person ergreifen muss. Dabei besteht zunächst eine allgemeine Pflicht zum Ergreifen aller physischen, technischen und verwaltungsspezifischen Massnahmen, die zur Verhinderung von Datenverlust, -diebstahl, -verbreitung, -verfälschung oder –zerstörung notwendig sind (Art. 29 PIPA), die in einer Präsidialverordnung konkretisiert wird. Ganz allgemein soll Information so bearbeitet werden, dass das Risiko von Verletzungen der Privatsphäre möglichst klein gehalten werden (Art. 3 Abs. 6 PIPA) und soweit möglich soll versucht werden, Daten anonym zu bearbeiten (Art. 3 Abs. 7 PIPA)

Im Weiteren muss die datenverarbeitende Person die im Unternehmen geltende allgemeine Datenschutzstrategie (***privacy policy***) annehmen und veröffentlichen, welche insbesondere den Zweck, die Bearbeitungsdauer, die allfällige Weitergabe an Drittpersonen sowie die Rechte und Pflichten der berechtigten Personen ausführt (Art. 30 PIPA). Daneben ist auch eine für die Datenbearbeitung zuständige Person (***privacy officer***) zu ernennen (Art. 31 PIPA).

Öffentliche Institutionen müssen die Datensammlung **registrieren** (Art. 32 PIPA) und ein ***Privacy Impact Assessment*** durchführen (Art. 33 PIPA), welches ebenfalls registriert wird. Das Privacy Impact Assessment ist eine vom Leiter der öffentlichen Institution durchzuführende Analyse der Risikofaktoren bezüglich der Verletzung von Rechten der betroffenen Personen. Die Analyse hat ausserdem die Zahl der bearbeiteten Daten, deren Teilung mit Drittpersonen sowie allfällige weitere Angaben zu behandeln (Art. 33 Abs. 2 PIPA). Weitere Einzelheiten sind auf Verordnungsstufe geregelt.

Private Institutionen sollen[65] ein Privacy Impact Assessment durchführen, wenn eine grosse Wahrscheinlichkeit der Verletzung von persönlichen Informationen besteht (Art. 33 Abs. 8 PIPA).

Schliesslich müssen alle datenverarbeitenden Personen die betroffenen Personen informieren, wenn sie davon Kenntnis erhalten, dass persönliche Informationen nach aussen gedrungen ist (**Datenleck**). Dabei muss die Art der betroffenen Information, der Zeitpunkt und die Art des Lecks, alle zur Schadensminderung notwendigen Informationen, die ergriffenen Massnahmen sowie Kontaktpunkte für Schadensmeldungen mitgeteilt werden (Art. 34 Abs. 1 PIPA). Die datenbearbeitende Person hat zudem eine Schadensminderungspflicht (Art. 34 Abs. 2 PIPA). Vorkommnisse, die mehr als 10'000 Personen betreffen[66], müssen zudem dem Innenministerium mitgeteilt werden (Art. 34 Abs. 3 PIPA).

---

64 Ausgenommen sind registrierte Datensammlungen im öffentlichen Sektor und die Gefahr für Drittpersonen.

65 Die englische Übersetzung spricht hier von « shall make efforts in a positive way to conduct ».

66 Art. 40 Abs. 3 Enforcement Decrees to Personal Information Protection Act.

4. Big Data, Profiling, Internet of Things

Gemäss den Ausführungsbestimmungen zum Netzwerk Gesetz[67] kann die *Korea Communication Commission* zum Schutz der persönlichen Information der Nutzer nach einem vorgehenden Konsultationsverfahren Empfehlungen in Form von Richtlinien erlassen. Dies erlaubt eine relativ schnelle Reaktion auf technische Entwicklungen im IT Bereich, wenn auch ohne formelle bindende Wirkung.

Am 23. Dezember 2014 hat die Korea Communication Commission nach einer relativ kontroversen Konsultationsphase[68] eine **Richtlinie im Bereich der Big Data** verabschiedet.[69] Diese sieht erstens eine weitgehende **De-Identifizierung** als Voraussetzung jeglicher Big-Data – Verarbeitung (Sammlung, Speicherung und Analyse) oder Übermittlung vor, wobei insbesondere öffentlich zugängliche persönliche Information und andere Internetbenutzungsdaten gemeint sind. Erfasst werden «Kodes, Buchstaben, Töne und Bilder», aber auch Internet Log Information und Aufzeichnungen über Transaktionen. Für die De-Identifizierung (durch Zerstörung, Pseudonymisierung, Kategorisierung, etc.) scheint die National Information Society Agency technische Unterstützung zu gewährleisten. Nach Durchführung ist die Zustimmung der betroffenen Person nicht mehr nötig, aber diese kann sich der entsprechenden Bearbeitung dennoch widersetzen. Zweitens haben die Kommunikations- und Informationsdienstleister eine Verpflichtung zur **Transparenz**: im Rahmen ihrer *Privacy Policy* müssen sie bekannt machen, dass Big Data Verarbeitung erfolgt, mit welchem Zweck sie erfolgt sowie aus welchen Quellen die Daten erhoben werden. Sie müssen die Betroffenen auch über ihr Recht informieren, die Unterlassung der Verarbeitung ihrer persönlichen Daten zu verlangen. Drittens sollen Daten sofort **zerstört** oder erneut de-identifiziert werden, wenn sie im Rahmen der Verarbeitung insbesondere durch Kombination mit anderen Daten **re-identifizierbar** werden. Viertens soll die Bearbeitung von öffentlich gemachten Daten zum Zweck der **Erzeugung sensibler Information** (z.B. die Ideologie, politische Meinungen, Religion) nicht erlaubt sein, ausser es besteht eine spezifische gesetzliche Grundlage oder eine ausdrückliche Zustimmung des Betroffenen. Fünftens müssen die IT- und Kommunikationsdienstleister gewisse **technische und organisatorische Sicherungsmassnahmen** für ihre Datenverarbeitungssysteme ergreifen. Dies beinhaltet insbesondere Zugangskontrollen und Antivirus-Software. Damit sollen auch die de-identifizierten Daten geschützt werden. Die Richtlinie soll den Dienstleistungserbringern zeigen, wie Big Data Verarbeitung im Rahmen des gesetzlichen und regulatorischen Rahmens möglich ist, und damit die Big Data Dienstleistungen unterstützen. Nach Meinung verschiedener Kommentatoren erzielen sie ein Gleichgewicht zwischen Datenschutzanliegen und Technologieunterstützung.[70]

---

67 Art. 3 des Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, verfügbar in englischer ÜBersetzung unter http://english.msip.go.kr/english/msipContents/contents.do?mId=Mjc5.

68 So scheint die Personal Information Protection Commission einen Entwurf der Richtlinie als mit Datenschutzbestimmungen unvereinbar angesehen zu haben, s. den Beschrieb der Big Data Guideline auf KoreanLii, verfügbar unter http://www.koreanlii.or.kr/w/index.php/Big_Data_Guideline.

69 Guideline for Big Data Personal Information Protection.

70 Angesichts der Nicht-Verfügbarkeit der englischen Übersetzung der Big Data Richtlinien beruhen die Informationen über die Richtlinien auf folgenden Quellen: KoreanLii, Big Data Guideline, zit.; Bloomberg BNA, The South Korean Communications Commission's Guidelines on Data Protection for Big Data, World Data Protection Report Vol 15 (2), February 2015; Shin & Kim, Guidelines for Protection of Big Data Personal Information, Legal Update, January 2015, verfügbar unter http://www.shinkim.com. C. O'Donoghue & P. Thomas, South KoreanCommunications Commission Releases Guidelines on Data Protection for Big Data, ReedSmith Technology Law Dispatch, 23.02.2015, verfügbar unter http://www.technologylawdispatch.com.

Das in der Big Data Richtlinie erwähnte Verbots der Erzeugung sensibler Information ist soweit ersichtlich das einzige Anzeichen, dass für **Profiling** Grenzen bestehen. Eine spezifischere Regulierung besteht soweit ersichtlich nicht.

Die Entwicklung des **Internet of Things** wird in Südkorea aktiv unterstützt.[71] Auf regulatorischer Eben sind diesbezüglich im Grundsatz ein liberaler Ansatz verfolgt, wobei gerade hier der Grundsatz des «privacy by design» angewendet werden soll.[72] Dies scheint dem allgemeinen Trend zu entsprechen.[73] Soweit ersichtlich bestehen keine zugänglichen Informationen über konkretere regulatorische Massnahmen diesbezüglich

Schliesslich sind zwei weitere Bereiche zu erwähnen, die Südkorea ausdrücklich geregelt hat. Erstens ist gemäss Art. 50 ff. des Netzwerkgesetzes das entgeltliche (for profit) Übermitteln von **Werbeinformationen** grundsätzlich nur mit Zustimmung der empfangenden Person zulässig. Zweitens hat Südkorea 2015 ein Gesetz zum **Cloud Computing** verabschiedet.[74] Neben verschiedenen Massnahmen zur Förderung des Cloud Computing verpflichtet das Gesetz die Cloud Dienstleister – aber auch Cloud Computing benutzende Kommunikationsdienstleister – dazu, Benutzer auf Anfrage über den Staat zu informieren, in welchem die diese betreffenden Informationen gespeichert werden (Art. 26). Zudem enthält das Gesetz eine Datenschutzbestimmung (Art. 27). Gemäss dieser Bestimmung ist die Zustimmung für die Datenweitergabe an Drittpersonen oder die Datenbearbeitung für andere Zwecke als die ursprüngliche Dienstleistung grundsätzlich erforderlich, wobei bei Änderungen diesbezüglich eine Informationspflicht bezüglich verschiedener definierter Aspekte (Identität der Drittperson, Zweck, Indikation der Information, Zeit, Information über Möglichkeit der Zustimmungsverweigerung) besteht.

5. Massnahmen zur Förderung von privacy by design / privacy by default

Verschiedene oben (3.) ausgeführte Grundsätze im PIPA, insbesondere Art. 3 Abs. 6 und 7 und 29 PIPA, setzen den Grundsatz der «privacy by design» in gewissem Sinn um (Grundsatz der anonymen Datenbearbeitung, Grundsatz des kleinstmöglichen Risikos für Verletzungen der Privatsphäre, Pflicht zum Ergreifen von Massnahmen zur Verhinderung von Datenverlust). Im Bereich des *Internet of Things* wird der Grundsatz ausdrücklich angesprochen (s. oben, 4.). Informationen über andere Massnahmen diesbezüglich liegen soweit ersichtlich nicht in zugänglicher Sprache vor.

6. Datenportabilität

Soweit ersichtlich bestehen in Südkorea bislang keine Vorschriften zur Datenportabilität.

---

71 S. BBC, 05.07.2016, South Korea Launches first internet of things network, verfügbar unter http://www.bbc.com/news/technology-36710667; zur Rolle und Vision des Staates diesbezüglich siehe z.B. den Master Plan for Building the Internet of Things des Ministry of Science, ICT and Future Planning, vom 08.05.2014, verfügbar unter http://www.kiot.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf; s. auch DataGuidance, South Korea: IoT roadmap focuses on security by design, 13.11.2014, verfügbar unter www.dataguidance.com.

72 Master Plan, zit., S. 11 sowie S. 10.

73 S. ITU, Regulation and the Internet of Things, GSR discussion paper, 2015, S. 25.

74 Act on the Development of Cloud Computing and Protection of ist Users, Act 13234, 27.03.2015.

C. JAPAN[75]

Einführung

Die japanische Datenschutzgesetzgebung ist eng mit der Entwicklung des **nationalen Identifikationssystems** (ein zentrales Einwohnerregister) verbunden: das Datenschutzgesetz von 2003 sowie Änderungen 2013 sind mit der Entwicklung entsprechender Systeme verbunden[76]. Das Datenschutzgesetz von 2003 (*Act on the Protection of Personal Information - APPI*)[77] enthält Grundprinzipien, die sowohl auf den öffentlichen als auch auf den Privatsektor anwendbar sind. Daneben bestehen einige lediglich auf den öffentlichen Sektor anwendbare Gesetze.[78] Zudem scheinen verschiedene Vorschriften nur in (unübersetzten) Richtlinien enthalten, und der Selbstregulierung (s. dazu auch 2.) kommt erhebliche Bedeutung zu.[79]

Im Jahr 2015 wurden wesentliche Änderungen in der Datenschutzgesetzgebung verabschiedet, welche u.a. den Anwendungsbereich des Datenschutzgesetzes auf alle privaten Organisationen ausweitet und eine einzige Datenschutzbehörde, die *Personal Information Protection Commission*, schafft[80]. Die technologische Entwicklung und insbesondere Big Data waren ein wesentlicher Grund für die Änderung.[81] Das revidierte Gesetz wurde am 9. September 2015 verkündet und tritt innert 2 Jahren danach in Kraft, wobei die neue Behörde bereits auf den 1. Januar 2016 ihre Tätigkeiten aufnimmt (s. unten, 2.).[82] Aufgrund des Zwecks des vorliegenden Gutachtens werden die folgenden Ausführungen in erster Linie auf das in inoffizieller englischer Übersetzung verfügbare revidierte Recht (*Amended Act on the Protection of Personal Information* - AAPPI[83]) Bezug nehmen.[84]

---

75 Dieser Bericht beruht auf den am Schweizerischen Institut für Rechtsvergleichung sowie online vorwiegend in englischer Sprache verfügbaren Informationen.

76 Greanleaf, S. 231 ff.; H. Murakami, La protection des données personnelles en droit public japonais, in B. Fauvarque-Cosson & Y. Ito, L'Information. VIIIe Jounrées juridiques franco-japonaises, Société de légilation comparée, Paris 2012, S. 69 ff., S. 71.

77 Act 57 of 2003; die japanische Gesetzgebung ist in inoffizieller englischer Übersetzung verfügbar auf der von der Regierung betreibenen Website http://www.japaneselawtranslation.go.jp/. Die Übersetzung des Act on Personal Information Protection berücksichtigt Änderungen bis 2009.

78 Act on Protection of Personal Information Held by Administrateive Organs sowie Act on the Protection of Personal _Information Held by Incorporated Administrative Agencies; letzterer ist nicht in englischer Übersetzung verfügbar, scheint aber ähnliche Grundsätze wie der erstere zu enthalten, s. Greenleaf, Asian Data Privacy Laws, zit., S. 234 sowie zu den Unterschieden zwischen Regelung des öffentlichen und privaten Sektors (vor der Reform von 2014: Murakami, zit., S. 74 ff..

79 Murakami, zit., S. 88 f. und 94.

80 Vorher war das Gesetz insbesondere nicht auf Firmen (« entities ») anwendbar, welche angesichts des Umfangs und die Art der Datenbearbeitung nur ein kleines Risiko für die Verletzung individueller Rechte darstellten, wobei dies gemäss Verordnung bei Unternehmen der Fall ist, welche Daten von nicht mehr als 5'000 identifizierbaren Personen bearbeiten; s. Art. (2) (3) (v) APPI und dazu Greenleaf, Asian Data Privacy Laws, zit., S. 239

81 S. Personal Information Protection Commission, Outline of the Amended Personal Information Protection Act, verfügbar unter http://www.ppc.go.jp/en/legal/ (11.07.2016).

82 Internetseite der *Personal Information Protection Commission*: http://www.ppc.go.jp/en (11.07.2016), s. auch Länderbericht Japan in DLA Piper, Data Protection Laws of the World, S. 216 ff., verfügbar unter *http://dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all* (29.01.2016), S. 217.

83 Verfügbar auf der Internetseite der Datenschutzbehörde : http://www.ppc.go.jp/en/legal/ (11.07.2016).

84 S. zum 2012 geltenden rechtlichen Rahmen den Bericht der Law Library of Congress, Online Privacy: Japan, verfügbar unter https://www.loc.gov/law/help/online-privacy-law/japan.php (10.07.2016) sowie H. Murakami, La protection des données personnelles en droit public japonais, in B. Fauvarque-

Im internationalen Vergleich galt das Level des Datenschutzes in Japan vor der Reform eher tief,[85] nähert sich aber mit der Revision etwas mehr dem europäischen Niveau an.[86] Auffallend sind im Vergleich ebenfalls die verschiedenen Arten von Daten und deren unterschiedliche rechtliche Regelung. So wird bis zum Inkrafttreten des neuen Rechts, die Sozialversicherungs- und Steuernummer gesondert geregelt und von einer spezifischen Behörde überwacht. Das neue Recht sieht drei Arten von Daten vor, deren Bearbeitung mindestens teilweise unterschiedlich geregelt ist: persönliche Daten, sensible persönliche Daten und anonymisierte Daten.

1. Aufsichtsbehörde

Bis Ende 2015 bestand in Japan keine allgemeine Aufsichtsbehörde im Bereich des Datenschutzes. Zwar wurde auf Anfang 2014 die *Specific Personal Information Protection Commission* geschaffen, doch hatte diese lediglich Zuständigkeiten im Zusammenhang mit der Steuer- und Sozialversicherungsnummer[87]. Die Aufsichtsfunktion für die anderen Belange wurde (und werden weiterhin) von den für den jeweiligen Bereich zuständigen Ministerien wahrgenommen.[88] Auch lokale Regierungen haben entsprechende Befugnisse, wobei hier für die Behandlung von Beschwerden ein Mediationsverfahren vorgesehen werden sollte (Art. 13 APPI).[89]

Seit 2016 besteht eine eigene Datenschutzbehörde, die ***Personal Information Protection Commission*** (PIPC). Gemäss dem neuen Recht wird sie Aufsichtsfunktionen, regulatorische Funktionen und schlichtende Funktionen haben, wobei ihr in diesem Rahmen auch Untersuchungsbefugnisse zustehen (Recht auf Auskunft, Inspektionen, s. Art. 40 AAPPI).[90] Zudem ist sie akkreditierende Behörde für private Datenschutzorganisationen (s. unten).[91] Ab Inkrafttreten des AAPPI 2017 werden die Aufsichtsbefugnisse sowie die schlichtende Funktion alle Bereiche des Datenschutzes umfassen, vorerst sind sie auf den Gebrauch der persönlichen Identifikationsnummer im staatlichen Verkehr (MYNUMBER) beschränkt.[92] Die Kommission untersteht administrativ dem Premierminister, doch der

---

Cosson & Y. Ito, L'Information. VIIIe Jounrées juridiques franco-japonaises, Société de légilation comparée, Paris 2012, S. 69 ff.

85 So Greenleaf, Asian Data Privacy Laws, zit., S. 263 ff.

86 G. Greenleaf, Japan: Towards international standards – except for 'big data', UNSW Law Reserach Paper No 2015-51, p. 3.

87 Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure, 2013 ; das Gesetz spricht von individuellen Daten, welche die auf Grund des Einwohnerregisters erzeugte individuelle Nummer enthalten (Art. 2 Ziff. 5); die Behörde ist in Art. 36 bis 57 geregelt; s. dazu auch Greenleaf, Asian Data Privacy Laws, zit., S. 236 f.

88 die Art. 9 und 10 APPI sehen hier sehr vage eine „Verantwortung" des Staates zur Beaufsichtigung und zur Sicherstellung der Behandlung von Beschwerden vor; bis zum Inkrafttreten des modifizierten Gesetzes bleibt der Zuständigkeitsbereich der Ministerien erhalten, s. Personal Information Protection Commission, Outline of the Amended Personal Information Protection Act, verfügbar unter http://www.ppc.go.jp/en/legal/ (11.07.2016), S. 7.

89 „In order to ensure that any complaint arising between a business operator and a person about the handling of personal information will be handled appropriately and promptly, a local government shall endeavor to mediate the processing of complaints and take other necessary measures.

90 Art. 61 AAPPI nennt die Formulierung einer «Basic Policy», Aufsicht und Mediation bei der Bearbeitung von persönlichen Daten sowie von besonderen Personendaten; s. Website : http://www.ppc.go.jp/en/ (04.02.2016) sowie http://www.ppc.go.jp/en/aboutus/roles/ .

91 Art. 61 AAPPI sowie

92 So Personal Information Protection Commission, Outline of the Amended Personal Information Protection Act, verfügbar unter http://www.ppc.go.jp/en/legal/ (11.07.2016), S. 7.

Vorsteher sowie die 8 Mitglieder üben ihr Amt unabhängig aus und können grundsätzlich[93] nicht gegen ihren Willen abgesetzt werden.[94]

Zwei weitere Institutionen sind im Zusammenhang mit der Aufsichtsbehörde zu erwähnen. So können **private Datenschutzorganisationen** nach Akkreditierung durch die *Personal Information Protection Commission* (PIPC) gewisse Aufgaben gegenüber ihren Mitgliedsunternehmen[95] übernehmen. Dies beinhaltet insbesondere das Behandeln von **Beschwerden** gegenüber den Unternehmen, das Erteilen von **Informationen** zur besseren Durchsetzung des Datenschutzes oder andere Unterstützung bei der **Umsetzung** der Datenschutzgrundsätze (Art. 37 und Art. 47 ff. AAPPI).[96] Sie können auch Richtlinien für die betroffenen Unternehmen verfassen, welche der PIPC mitzuteilen sind und von dieser publiziert werden (Art. 53 AAPPI). Der Mechanismus ermöglicht also eine gewisse Selbstregulierung unter staatlicher Aufsicht.

Im öffentlichen Sektor ist zudem auf das Bestehen des *Information Disclosure and Personal Information Protection Review Board* hinzuweisen, welches den individuellen Datenschutz bei Transparenzanfragen gewährleisten soll.

2. Rechte der Betroffenen[97]

Anders als Datenschutzgesetze in anderen Staaten sieht das neue Datenschutzgesetz (AAPPI) in Japan in der Struktur und auch im Grundsatzartikel (Art. 3 AAPPI) keine Rechte der Betroffenen vor, sondern ist nach Pflichten und Verantwortlichkeiten der Datenbearbeiter formuliert. Daraus ergeben sich teilweise nur Anzeichen für Rechte der Betroffenen. Der Grundsatzartikel (Art. 3 AAPPI) sieht eine zurückhaltende Datenbearbeitung nach dem Grundsatz der individuellen Autonomie vor. Daraus lässt sich jedoch nicht ein Zustimmungserfordernis in allen Fällen ableiten. Dieses besteht im Privatsektor gemäss Art. 23 AAPPI für die Weitergabe von Informationen an Dritte oder gemäss Art. 17 AAPPI für die Erhebung von sensiblen persönlichen Daten (Informationen welche Diskriminierung oder Benachteiligungen nach Rasse, sozialem Status, Gesundheit, Strafregister bewirken können[98]), und auch dann nicht ohne Ausnahmen.[99]

Gewisse Pflichten der Unternehmen (*business operators*), welche Daten bearbeiten, führen aber durchaus zu Rechten der Betroffenen. So haben Betroffene das Recht, nach dem Zweck einer

---

93 Gemäss Art. 65 AAPII ist eine Absetzung nur bei Insolvenz, Verurteilung wegen Verletzung der Datenschutzgesetzgebung oder der Verurteilung zu einer Gefängnisstrafe, oder Unfähigkeit zur Amstausübung nach Meinung der Kommmissionsmehrheit möglich.

94 Art. 59 Abs. 2 und Art. 62 AAPII sowie Art. 65 AAPII.

95 Art. 51 AAPPI.

96 So gemäss der Website : http://www.ppc.go.jp/en/aboutus/roles/accredited_org/.

97 Die folgenden Ausführungen betreffen in erster Linie den Privatsektor. Im öffentlichen Sektor ist das neue Datenschutzgesetz zwar auch gültig, doch sieht dies lediglich vor, dass die Regierungen (auf nationaler und lokaler Ebene) die notwendigen Massnahmen ergreifen muss, um die richtige Datenbearbeitung gemäss den allgemeinen Prinzipien zu gewährleisten, so dass die Rechte und Interessen der Betroffenen geschützt werden (Art. 4 bis 6). Diese allgemeinen Ausführungen ermöglichen keine Aussagen über die Rechte der Betroffenen gegenüber den staatlichen Behörden.

98 Art. 2 Abs. 3 AAPPI.

99 Ausnahmen sind z.B. die Erhebung der Daten nach Gesetz oder Verordnung oder die Notwendigkeit der Information zum Schutz von Leben, körperlicher Integrität oder Eigentum der betroffenen Person bzw. der öffentlichen Gesundheit, wenn die Zustimmung nur schwierig erhalten werden kann; Art. 17 Abs. 2 lit. i bis vi, ähnliche Ausnahmen finden sich in Art. 23 Abs. 1 lit. i bis iv.

Datenbearbeitung (Art. 27 Abs. 1 lit. ii) zu fragen. Es besteht grundsätzlich[100] auch ein **Recht auf Auskunft** über persönliche identifizierende Daten, welche bearbeitet werden (Art. 28 AAPPI). In beiden Fällen kann das Unternehmen jedoch Kosten erheben (Art. 33 AAPPI). Zudem können Betroffene die **Korrektur** oder **Ergänzung oder Löschung von** falschen persönlichen (identifizierenden) Daten verlangen, worauf die datenbearbeitende Person die Vorwürfe abklären muss und bei Nichtentsprechen mit dem Antrag die betroffene Person informieren muss (Art. 29 AAPPI). Berechtigte können die Einstellung der Datenbearbeitung verlangen, sofern diese ohne Zustimmung dem ursprünglich vorgesehenen Zweck widerspricht, oder von Daten, die mit illegalen Mitteln erhalten wurden (Art. 30 Abs. 1 AAPPI). Einem entsprechenden Gesuch muss allerdings nicht entsprochen werden, wenn es hohe Kosten verursachen würde oder sonst schwierig ist und andere Massnahmen ergriffen werden (Art. 30 Abs. 2 APPI). Ein eigentliches Widerspruchsrecht gegen die Bearbeitung richtiger bzw. legal erhaltener Daten gibt es somit – auch unter neuem Recht – nicht.[101] Im Bereich der de-identifizierten Daten (s. dazu unten, 4.) sind soweit ersichtlich keine individuellen Rechte vorgesehen.

Die betroffene Person hat ein Recht, die oben erwähnten Ansprüche **auf dem Gerichtsweg** zu verfolgen, wenn das Unternehmen einem Ersuchen nicht innert zwei Wochen entsprochen hat oder dieses abgewiesen hat (Art. 34 AAPPI). In verfahrensmässiger Hinsicht sollen einerseits auf nationaler Ebene Beschwerdemechanismen eingeführt werden (Art. 9 AAPPI), andererseits nach Möglichkeit auf lokaler Ebene Schlichtungsverfahren angeboten werden (Art. 13 AAPPI[102]).

3. Pflichten der für die Datenbearbeitung verantwortlichen Personen[103]

Das neue Gesetz unterscheidet zwischen Pflichten von Unternehmen, welche **persönliche Daten** (*personal information*)[104] bearbeiten und Pflichten bei der Bearbeitung von **anonymisierten** Informationen. Diese rechtliche Zweiteilung, welche insbesondere die Big Data Verarbeitung in datenschutzrechtlicher Hinsicht ermöglichen soll, ist im internationalen Vergleich eine Ausnahme.[105] Auf die Vorgaben zur Anonymisierung wird eingehender unter 4. eingegangen, im Folgenden werden lediglich die Pflichten bei der Bearbeitung persönlicher Daten und anonymisierter Information behandelt.

Die Pflichten für die Bearbeitung persönlicher Daten sind relativ ausführlich geregelt (Art. 15 bis 35 AAPPI). Zunächst müssen die für Datenbearbeitung verantwortlichen Personen müssen den **Zweck der**

---

100 Neben den ähnlichen Ausnahmen wie nach Art. 17 und Art. 23, oben, reicht insbesondere bereits das Risiko einer ernsthaften Störung der unternehmerischen Aktivitäten.

101 Zum alten Recht: Greenleaf, Asian Data Privacy Laws, zit, S. 251.

102 « A local government must endeavor to provide mediation for complaint processing and take other necessary measures to ensure that any complaint arising between an enterprise and a person with regad to the handling of personal information is handled appropriately and promptly ».

103 Die folgenden Ausführungen betreffen in erster Linie den Privatsektor. Im öffentlichen Sektor ist das neue Datenschutzgesetz zwar auch gültig, doch sieht dies lediglich vor, dass die Regierungen (auf nationaler und lokaler Ebene) die notwendigen Massnahmen ergreifen muss, um die richtige Datenbearbeitung gemäss den allgemeinen Prinzipien zu gewährleisten, so dass die Rechte und Interessen der Betroffenen geschützt werden (Art. 4 bis 6). Die spezifischen Pflichten im öffentlichen Sektor lassen sich dabei nicht bestimmen, doch entsprechen sie in den Grundzügen wohl weitgehend denjenigen im Privatsektor

104 Gemäss Art. 2 Abs. 1 AAPPI geht es um Information, welche zur Identifizierung einer Person dienen kann (z.B. durch Name, Geburtsdatum, andere Beschreibung), auch durch Abgleich mit anderer Information, oder um Information welches individuelle Identifikationscode enthält.

105 So G. Greenleaf, Japan : Toward international standards – except for 'big data', UNSW Law Research Paper 2015-51, p. 6; vgl. allerdings den Ansatz in Südkorea, der dort jedoch nur in einer unverbindlichen Richtlinie vorgesehen ist.

Datenbearbeitung spätestens beim Erhalt der Daten so genau wie möglich offenlegen und Daten dürfen nur in diesem Rahmen bearbeitet werden (Art. 15 f. APPI und Art. 15 f. und Art. 18 AAPPI). Daten müssen rechtmässig (insbesondere nicht durch Täuschung) erworben werden (Art. 17 AAPPI), wobei das Einverständnis nur bei gewissen Daten ausdrücklich eingeholt werden muss (Art. 17 AAPPI, s. oben, 2.) – in den übrigen Fällen scheint das implizite Einverständnis zu genügen [106].

Die Unternehmen müssen die **Genauigkeit der Daten** aufrecht zu erhalten versuchen[107] und nach dem neuen Gesetz auch **zerstören**, sobald diese nicht mehr länger benötigt werden (Art. 19 AAPPI). Ganz allgemein sollen **Sicherheitsmassnahmen** zur Verhinderung von Datenbeschädigung oder –verlust ergriffen werden (Art. 20 APPI) und mit der Datenbearbeitung betraute Personen sind zu überwachen (Art. 21 f. APPI). In den meisten dieser Punkte entspricht das neue Recht weitgehend dem alten Recht.

Bei den Pflichten im Zusammenhang mit der **Weitergabe der Daten an Dritte** ist das neue Recht etwas ausführlicher als vorher. Die Weitergabe von persönlichen Daten an Dritte ohne Zustimmung ist auch nach neuem Recht nur in besonderen Fällen möglich (z.B. zum Schutz von Leib und Leben oder der Öffentlichen Gesundheit, oder im Rahmen der Zusammenarbeit mit öffentlichen Organen; Art. 23 APPI), wobei die Weitergabe dann möglich ist, wenn die betroffene Person (allenfalls via Website)[108] informiert wird und ihr die Möglichkeit gegeben wird, sich der Weitergabe zu widersetzen, und die *Personal Information Protection Commission* informiert wird (Art. 23 Abs. 2 bis Abs. 3 AAPPI). Nach neuem Recht ist die Weitergabe von persönlichen Daten an Dritte ausserhalb von Japan nur mit Zustimmung möglich, ausser das entsprechende Land weist gemäss der PIPC ähnliche Standards via Japan auf.

Das Gesetz selbst sieht keine Verpflichtung der für die Datenbearbeitung zuständigen Person vor, bei **Datenverlusten zu informieren**. Verschiedene Richtlinien scheinen aber eine Pflicht vorzusehen, die Behörden und die betroffenen Personen oder gar die Öffentlichkeit zu informieren.[109]

Bei der Bearbeitung **anonymisierter Information** sollen zunächst verschiedene Vorschriften sicherstellen, dass die betroffenen Personen nicht durch Kombination mit anderer Information oder durch Rückgängigmachen zerstörter Information identifiziert werden können (Art. 36 Abs. 5 sowie Art. 38 AAPPI). Daneben sieht das neue Recht die Pflicht vor, die notwendigen und angebrachten Massnahmen zur sicheren Bearbeitung der Information sowie zur angemessenen Bearbeitung zu ergreifen. Die Öffentlichkeit muss über diese Massnahmen informiert werden. Schliesslich müssen die Unternehmen Beschwerden im Zusammenhang mit der Schaffung und Bearbeitung de-identifizierter Information behandeln (all dies gemäss Art. 36 Abs. 6 und Art. 39 AAPPI). Angesichts der Unbestimmtheit der gesetzlichen Vorgaben ist zu erwarten, dass die *Personal Information Protection Commission* diese Pflichten spezifizieren wird.

4. Big Data, Profiling, Internet of Things

Soweit ersichtlich bestehen keine spezifische Massnahmen zu Profiling und zum Internet of Things – es scheinen die allgemeinen Grundsätze anwendbar.[110] Wie bereits erwähnt bezweckt jedoch das neue Gesetz durch die Einführung des Begriffs der anonymisierten Daten und verschiedener Pflichten diesbezüglich (s. oben, 3.) die Klärung und damit Ermöglichung der Rechtslage in Bezug auf Big Data

---

106 So zum geltendem REcht Greenleaf, Asian Data Privacy Laws, zit., S. 242.

107 « A business operator (...) must endeavor to keep the content of personal data accurate and up to date (...). »

108 So gemäss Greanleaf, Japan : Toward international standards, zit., S. 4.

109 Greenleaf, Asian Data Privacy Laws, zit., S. 246 ; DLA Piper, Japan, p. 219.

110 S. DLA Piper, Japan, S. 221.

Verarbeitung. Ein Kernpunkt der Regelung ist dabei die Definition des Begriffs der anonymisierten Daten. Das Gesetz definiert zwar einerseits anonymisierte Information als Information zu einem Individuum, welche so bearbeitet wurde, dass eine Identifikation der betroffenen Person nicht mehr möglich ist, indem Beschreibungen zu persönlichen Informationen (wie Name, Adresse, etc.) zerstört oder ersetzt werden oder die Identifikationscodes entfernt werden (Art. 2 Abs. 9 AAPPI). Bei der entsprechenden Anonymisierung sind die Vorgaben der *Personal Information Protection Commission* anzuwenden, auch bezüglich Sicherheit zur Verhinderung der Veröffentlichung der zerstörten persönlichen Information (Art. 36 Abs. 1 und 2 AAPPI). Dies ist insbesondere relevant, da Experten hier die Effektivität der entsprechenden Massnahmen durchaus bezweifeln könnten.[111] Die Regelung bezweckt also vor allem Rechtssicherheit.

Bei der Schaffung der anonymisierten Information bestehen auch verschiedene Informationspflichten. So muss angegeben werden, welche Information betreffend eines Individuums in der anonymisierten Information beinhaltet ist und wie diese veröffentlicht wird (Art. 36 Abs. 3 und 4 AAPPI). Auch hier wird die *Personal Information Protection Commission* genauere Regelungen zum Verfahren erlassen.

5. Massnahmen zur Förderung von privacy by design / privacy by default

Die Formulierung verschiedener Bestimmungen, welche angemessene Massnahmen im Zusammenhang mit der Bearbeitung von Daten verlangen (s. oben, 3.), lassen grundsätzlich Raum für die Konzepte der Privacy by design und privacy by default. Damit die Begriffe entsprechend ausgelegt werden, sind aber wohl Richtlinien der Personal Information Protection Commissioin erforderlich. Soweit ersichtlich sind diese noch nicht ergangen.

6. Datenportabilität

Soweit ersichtlich enthält das japanische Recht – auch das neue Recht – keine Vorschriften, welche die Portabilität der Daten verlangen würden.

111 Greanleaf, Japan : Toward international standards, S. 5.

D. NEUSEELAND

Das neuseeländische Datenschutzgesetz von 1993 (Privacy Act 1993) ist auf den öffentlichen und den privaten Sektor anwendbar. Die Aufsichtsbehörde (Privacy Commissioner) kann dazu für verschiedene Sektoren Codes of Practice erlassen, welche für die betroffenen Sektoren die Funktionsweise des Gesetzes erheblich beeinflussen können. Entsprechende Codes of Practice bestehen im Justizsektor, zu Gesundheitsinformationen, zu Kreditinformationen sowie zu mehrjährigen Informationen erlassen. Es gibt auch einen Code of Practice zu Telekommunikationsinformation.[112]

Die Gesetzgebung wurde in den letzten Jahren kritisch geprüft und Reformbestrebungen sind im Gang.

Overview

Data protection in New Zealand is **principally governed by the Privacy Act 1993 (the "1993 Act")**.[113] Unlike the framework found in certain other countries, it does not operate as a code, nor does it preclude the operation of the common law. Although it describes itself as promoting and protecting individual privacy, it also **recognises the existence of competing interests** which may, on occasion, outweigh an individual's privacy claim and justify disclosure to their parties.[114]

The 1993 Act controls how 'agencies' collect, use, disclose, store and give access to 'personal information'. **Almost every person or organisation that holds personal information is an 'agency'**, including government departments, companies of all sizes, religious groups, schools and clubs. **At its core are 12 privacy principles (the "IPPs")** covering the collection of personal information, storage and security, requests for access to and correction of personal information, accuracy of personal information, retention of personal information, use and disclosure of personal information and using what are known as 'unique identifiers'.[115]

A Privacy Commissioner **(also known as the "Office of the Privacy Commissioner" or "OPC")** is established as privacy regulator under the 1993 Act, and has **numerous functions** in relation to data protection, including an educational role, investigating complaints and engaging in policy developments. Given the generality of the IPPs, the 1993 Act also allows the Commissioner to **issue codes of practice which apply the IPPs within particular industries**, sectors or contexts, such as health, telecommunications and credit reporting.

As open-ended principles, the **IPPs have the merit of allowing flexibility** and provide the Commissioner with discretion to be applied on a case-by-case basis. In the absence of reference to specific technologies, they are also considered to be "**technology-neutral**". On the other hand, this does however preclude the operation of a system of precedent and results in different interpretations and applications of principles by agencies. Moreover, there has more recently been recognition of the way in which **technological changes have led to changes to the way data is stored, retrieved and transmitted digitally** and that large amounts of harm can be caused to large numbers of individuals by

---

112 S. die Website des Privacy Commissioner : https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/ (04.02.2016).

113 Privacy Act 1993, available at http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html (11.04.2016).

114 Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand*, Brookers Limited, 2010, Wellington, p.50.

115 Privacy Commissioner website, *Privacy Act and codes – Introduction*, available at https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/ (19.05.2016).

a single breach, rather than harm to a single individual. At the same time, the Government has demonstrated a commitment to **embracing the information and insight offered by Big Data**.

In **2006**, the New Zealand Law Commission was asked by the Government to conduct a **review of New Zealand's privacy framework**. The fourth and final stage, completed in 2011, recommended that a new Privacy Act be introduced, but that the **principles-based approach be retained**. Proposals provisionally accepted on behalf of the Government, in 2014, to amend the privacy framework, are numerous, but principally aim to **strengthen the Privacy Commissioner's investigation and enforcement powers**, to better **protect cross-border information flows** and to place **stricter requirements** on agencies to **report privacy breaches**. There are **no proposed legislative amendments targeted at specific technologies** or digital phenomena. Proposed measures designed to tackle technological challenges focus instead on **improved education and guidance** for agencies.

There have been no particular developments in the reform program since the Justice Minister confirmed in May 2014 that the Government would be proceeding with reforms to the 1993 Act. However, it was finally **announced by the Minister on 11th May 2016** that a draft Privacy Act would be published for consultation before the end of 2016, with a view to **introducing the Act in Parliament in 2017**.[116]

1. Supervisory Authority

1.1. Current law

In New Zealand, the public authority with responsibility for overseeing data protection is the **Privacy Commissioner**.[117] The Privacy Commissioner's numerous privacy-enhancing functions are set out in section 13(1)(a)-(u) of **the 1993 Act**. Other functions, referred to in other parts of the 1993 Act, include the approval of codes of practice under Part 6, overseeing a complaints process under Part 8, and consultation with the Ombudsmen, Health and Disability Commissioner and Inspector-General of Intelligence and Security under Part 12.

The Commissioner himself considers his **core functions** as the following:[118]

- *Legislation and policy:* commenting on legislative, policy or administrative proposals that impact on individual privacy, while having due regard to competing interests (in 2007/2008, some 260 legal and policy projects were addressed);
- *Compliance*: receiving, investigating and encouraging settlement of about 600 complaints annually from the public about breaches of privacy in both the private and public sectors; issuing case notes;
- *Education and awareness*: promoting understanding of the Information Privacy Principles ("IPPs"), set out in the 1993 Act. Activities include an enquiries helpline (more than 7000 calls per year), website, training workshops and seminars (94 in 2007/8), publications, speeches and responses to media enquiries (150 per year);

---

116 Beehive.govt.nz, *Opening address to the Wellington Privacy Forum*, 11th May 2016, available at https://www.beehive.govt.nz/speech/opening-address-wellington-privacy-forum (19.05.2016).

117 Office of the Privacy Commissioner, website available at https://www.privacy.org.nz/ (11.04.2016).

118 More recently set out in the Privacy Commissioner, *Statement of Intent 1 July 2014 – 30 June 2018*, available at https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/SOI-Office-of-the-Privacy-Commissioner-2014-18-FINAL.pdf (12.04.2016), p.3; also referred to in Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand*, *op. cit.*, pp.62-63.

- *Information matching programmes*:[119] oversight and monitoring of all government information matching programmes (of which there were 85 authorised, including 48 active, matching programmes in February 2009);
- *Codes of Practice*: issuing codes which modify the IPPs for application in particular industries or sectors;
- *International aspects*: working and sharing knowledge with counterparts in other jurisdictions, especially in the Asia-Pacific region; and
- *Other statutory functions*: these include monitoring compliance with the public register privacy principles; monitoring developments in data processing and computer technology for their impact on individual privacy; monitoring the use of unique identifiers, and reporting to the Prime Minister from time to time on the results of such monitoring; reporting on matters that require government attention or action, including any legislative or administrative or other action.

The **independence and authority of the Privacy Commissioner** is, as with officers of Parliament, defined in statute, and there is a statutory obligation on the Commissioner to act independently in performing his or her statutory functions and duties.[120] From a constitutional perspective, the Office of the Privacy Commissioner is, according to the 1993 Act, **constituted as an independent Crown Entity**.[121] This means that the Office is independent of government policy, although in this case, monitored by the Ministry of Justice.[122] The OPC itself describes this as meaning that the Privacy Commissioner is **independent of the Executive**[123] and is **free from influence when investigating complaints**, including those against Ministers or their departments.[124]

As with other independent Crown entities, the **appointment of the Privacy Commissioner**, as a member of an independent Crown entity is made by the Governor-General,[125] on the recommendation of the Minister of Justice.[126] Such recommendation must be made in accordance with criteria set out by statute, namely that the person recommended must, in the opinion of the Minister, have the appropriate knowledge, skills and experience to assist the entity to achieve its objectives and perform its functions, and that such appointment must further take into account the desirability of promoting diversity in the membership of Crown entities.[127]

---

119 "Information matching" refers to a comparison of one set of records with another, to find records in both sets of data that relate to the same person. For more detail, see Privacy Commissioner website, *Information matching overview*, available at https://www.privacy.org.nz/information-sharing/overview-matching/ (12.04.2016).

120 Privacy Act 1993, *op. cit.*, section 13(1A).

121 Privacy Act 1993, *op. cit.*, section 12.

122 Crown Entities Act 2004, section 7, available at http://www.legislation.govt.nz/act/public/2004/0115/latest/DLM329641.html#DLM329641 (12.04.2016).

123 The Executive may be considered as the branch of government that is responsible for the day-to-day management of the State.

124 Privacy Commissioner, *Annual Report 2014*, available at https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-annual-report-2014-web3.pdf, p.25.

125 The "Governor-General" refers to the officer appointed to represent the Queen in the governing of New Zealand, as an independent realm.

126 Crown Entities Act 2004, section 28, available at http://www.legislation.govt.nz/act/public/2004/0115/latest/DLM329954.html#DLM329954 (12.04.2016).

127 *Ibid*, section 29.

The Privacy Commissioner is **mainly funded through revenue from the Crown**,[128] restricted in its use for the purpose of the Privacy Commissioner in meeting its objectives. Financial targets of the OPC are agreed with the Minister of Justice at the beginning of the year, with Crown funding reflecting this. This is otherwise known as an "appropriation" from the Ministry of Justice's budget.[129] The OPC's independence is therefore limited by its reliance on public funding. The Privacy Commissioner itself nevertheless states in its annual report that it **considers there are no conditions attached to the funding** and that it is, *"recognised as revenue at the point of entitlement."*[130]

As referred to above, **one of the key functions of the Privacy Commissioner is to issue codes of practice** which apply the IPPs within particular industries, sectors or contexts. Every agency (whether large or small, whether in the private or public sector) is required to have at least one privacy officer whose responsibilities include encouraging compliance by the agency with the IPPs, dealing with privacy requests, working with the Commissioner over investigations and otherwise ensuring compliance with the 1993 Act.[131] In light of the generality of the IPPs set out at Part 2 of the 1993 Act, it is helpful to privacy officers that Part 6 of the 1993 Act allows the Commissioner to issue such codes of practice in order to adapt the IPPs to a particular industry and to modify their application, for example, by prescribing more stringent or less stringent standards.

The first Code of Practice was the Health Information Privacy Code which applies to the health sector, and which adapts the twelve IPPs by allowing instances of non-compliance through permitted exceptions and ensuring that patients (or their representatives) control as far as possible the collection and use of information about their health status and treatment, consistent with the 1993 Act.[132] **Other Codes of Practice** are: the Credit Reporting Privacy Code,[133] the Justice Sector Unique Identifier

---

128 The "Crown" refers to the office in which supreme power is legally vested, as filled by the sovereign (in New Zealand, this being the British monarch of the day). In practice, it is the minister, and not the sovereign, who today carries out common law powers and is said to be the Crown when so doing. See Jonathan Law (ed.), *Oxford Dictionary of Law*, 8th ed., Oxford 2015, p. 164.

129 See Privacy Commissioner, *Statement of Performance Expectations 1 July 2015 – 30 June 2016*, available at https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/SPE-Office-of-the-Privacy-Commissioner-2015-16-FINAL.pdf, p.5.

130 Privacy Commissioner, *Annual Report 2015*, available at https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-annual-report-2015.pdf (12.04.2016), p. 36.

131 Privacy Act 1993, *op. cit.*, section 23. Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand*, *op. cit.*, p.66.

132 See Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand*, *op. cit.*, p.67 and Privacy Commissioner website, *Codes of Practice*, available at https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/ (13.04.2016).

133 Privacy Commissioner, *Credit Reporting Privacy Code 2004,* available at https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/CRPC-Including-Amendments-2-to-5-and-7-to-10-5-November-2015.pdf (13.04.2016). This Code applies to "credit reporters", defined as an agency that carries on a business of reporting to other agencies, for payment, information relevant to the assessment of the creditworthiness of individuals.

Code,[134] the Superannuation Schemes Unique Identifier Code[135] and the Telecommunications Information Privacy Code.[136]

The **legal status of such codes of practice** is that they are considered to be what are known as "regulations", enforceable through the Privacy Commissioner and the Human Rights Review Tribunal ("HRRT"),[137] but not usually through normal courts. Unlike Acts of Parliament (or statutes), considered to be primary legislation, *regulations* are the result of law-making powers delegated by Parliament to other persons or bodies.[138] The 1993 Act itself states that a **failure to comply with a code**, even though not a breach of any information privacy principle, shall otherwise be deemed to be a breach of an information privacy principle.[139] Given that principles featured in the codes, replacing certain of the information privacy principles, are styled as "rules" within certain codes of practice, it is nevertheless reported that there is **confusion about the legal status of such codes of practice** and whether such "rules" are binding, persuasive or merely informative.[140]

1.2. Proposed reforms

Some of the main changes to the data protection system featured in the **proposed reforms to the 1993 Act concern the functions of the Privacy Commissioner**, particularly the Commissioner's enforcement powers.

It is reported by the Minister of Justice that currently, the Privacy Commissioner only becomes aware of privacy breaches through voluntary notification, complaints and media reports.[141] Moreover, the Privacy Commissioner only has limited powers to help prevent breaches from occurring, or to take action if they do. Under the proposals for reform, a **system of mandatory reporting of data breaches**

---

134 Privacy Commissioner, *Justice Sector Unique Identifier Code 1998*, available at https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/JSUIC-Incorporating-Amendments-1-to-4-15-October-2015.pdf (13.04.2016). This Code applies to various public agencies, such as the Department of Corrections, the New Zealand Transport Agency, the Ministry of Justice, the Ministry of Transport, the Police, the Ministry of Social Development and the Registrar of Motor Vehicles.

135 Privacy Commissioner, *Superannuation Schemes Unique Identifier Code 1995*, available at https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/SSUIC-incorporating-Amendment-No-1-15-October-2015.pdf (13.04.2016). This Code applies to trustees, administration managers, investment managers, actuaries and insurers or benefit providers to superannuation schemes (in other words, retirement or other benefits funds in relation to accidents, disability, sickness or death).

136 Privacy Commissioner, *Telecommunications Information Privacy Code 2003*, available at https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/TIPC-Incorporating-Amendments-3-and-4-15-October-2015.pdf (13.04.2016). This Code applies to information about an identifiable individual that is subscriber information, traffic information and the content of a telecommunication collected or held by telecommunications agencies, including (but not limited to) network operators, internet service providers and mobile telephone retailers.

137 The Human Rights Review Tribunal was set up to deal with claims relating to breaches of the Human Rights Act 1993, the Privacy Act 1993 and the Health and Disability Commissioner Act 1994. It may hear complaints about breaches of the Privacy Act 1993 only after a complaint has first been investigated by the Privacy Commissioner. See Ministry of Justice website, *Human Rights Review Tribunal*, available at http://www.justice.govt.nz/tribunals/human-rights-review-tribunal (13.04.2016).

138 See New Zealand Parliament website, *The role of the Regulations Review Committee*, available at http://www.parliament.nz/en-nz/features/00NZPHomeNews201204161/the-role-of-the-regulations-review-committee (13.04.20160.

139 Privacy Act 1993, *op. cit.*, section 53(b).

140 See Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand, op. cit.*, p.57

141 Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper*, 13 March 2014, available via: http://www.justice.govt.nz/publications/global-publications/r/reforming-the-privacy-act-1993 (13.04.2016).

will be introduced.[142] This will be accompanied by two enhancements to the Privacy Commissioner's powers of enforcement:

- The Commissioner will be **able to make urgent requests for information**, and the penalty for failures to comply with the Commissioner's requests (as a criminal offence) will be increased from $2,000 to $10,000.[143]

  Currently, the Commissioner can initiate his own investigations into any matter if it appears the privacy of an individual is, or may be, infringed. The Commissioner has compulsory information-gathering powers and can summon witnesses. The Commissioner does not however have the discretion to decrease the 20 working days' time frame within which agencies[144] have to comply.

- The Commissioner **will be able to issue compliance notices for breaches of the revised Act**. Compliance notices will require an agency to do something, or to stop doing something, in accordance with the Act. Such notices will be enforceable in the HRRT.

  Currently, the Commissioner can only make recommendations and has limited ability to act if he identifies wider concerns with systems or procedures, or if agencies are unwilling to comply.[145]

2. Rights of the persons concerned

2.1. Current law

Under the Information Privacy Principles ("IPP") set out at Part 2 of the 1993 Act, individuals have certain **rights in relation to the treatment of their personal information**:

- Under IPP 6, individuals are entitled **to confirmation of whether information is being held about them**, and to have access to it.
- Under IPP 7, individuals are entitled **to request correction of personal information**, and if it is not corrected, to insist that a statement is attached to the information showing that a correction was sought.[146]

The 1993 Act also provides that individuals who consider that they have suffered a breach of one or more of the IPPs, or indeed, anyone who alleges that any action is or appears to be an interference with the privacy of an individual, **may complain to the Privacy Commissioner**.[147]

---

142 See section 3 of this country report, below.

143 Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper, op. cit.*, para. 55.

144 "Agency" is the name given by the Privacy Act 1993 to individuals and organisations who, under equivalent English rules, "process" data. It can mean any person or body of persons, whether corporate or unincorporated, and whether in the public sector or private sector as well as government departments: Privacy Act 1993, *op. cit.*, section 2.

145 Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper, op. cit.*, paras. 59-61.

146 Privacy Act 1993, *op. cit.*, Part 2 and Part 5.

147 Privacy Act 1993, *op. cit.*, section 67(1).

It is also important to note that under New Zealand law, **breaches of the privacy of individuals may also give rise to justiciable rights** under the common law[148] tort of invasion of privacy, as well as under a range of other legislative provisions particular to the circumstances. Other **common law remedies** available from the courts include those relating to duties of confidentiality, negligence and contractual claims where contracts are breached as to data.[149] Protection under the tort of privacy[150] principally concerns the public disclosure of private facts about the complainant, while **legislation** includes: the Harmful Digital Communications Act 2015,[151] which provides for protection against harm caused by the posting of digital communications; section 92C of the Copyright Act 1994,[152] which provides a safe harbour that internet service providers are not liable for storing infringing material unless they are aware that the material infringes copyright and do not delete the material or prevent access to it as soon as possible; and the Harassment Act 1997,[153] under which the court has power to impose special conditions on restraining orders, which could extend potentially to the take-down of material that constitutes harassment.

The present report will, however, only focus on justiciable rights arising from alleged breaches of personal data and their right to complain to the OPC, as the designated supervisory authority.

Part 8 of the 1993 Act establishes a **complaints process**. This begins by requiring the Commissioner to respond to complaints. The Commissioner may investigate the complaint, or, decide to take no action in relation to the complaint where he is of the opinion that circumstances set out in section 71 apply.[154] In either case, the **Commissioner is required to respond to the complainant**.

For an interference with privacy to be found, **the individual needs to have suffered both a breach of a privacy principle and consequent type of harm** as set out in the 1993 Act, namely the action has caused or may cause loss, detriment, damage or injury to that individual, or has adversely affected or may adversely affect the rights, benefits, privileges, obligations or interests of that individual, or has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.[155]

In addition to a process of investigation, **provision is made for complaints to be dealt with by way of conciliation**. Given that one purpose of the 1993 Act is to change privacy-invasive practices, the conciliation process offers the chance to alert agencies to the need to change their systems and

---

148 "Common law" refers to those rules of law developed by the courts as opposed to those created by statute.

149 International Comparative Legal Guides, *New Zealand – Data Protection 2015*, contributed by Michael Wigley of Wigley & Company, available at https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/new-zealand (15.04.2016).

150 The tort of privacy as a public disclosure/private fact tort was only first recognised by the New Zealand Court of Appeal in 2005 as a new common law cause of action: *Hoskin v Runting* [2005] 1 New Zealand Law Reports 1 (Court of Appeal).

151 Harmful Digital Communications Act 2015, available at http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html (14.04.2016).

152 Copyright Act 1994, available at http://www.legislation.govt.nz/act/public/1994/0143/latest/DLM345634.html (14.04.2016).

153 Harassment Act 1997, available at http://www.legislation.govt.nz/act/public/1997/0092/latest/DLM417078.html (14.04.2016).

154 Privacy Act 1993, *op. cit.*, section 71 sets out a list of circumstances which the Commissioner may rely on in choosing not to take further action. These include: the length of time which has passed since the subject matter of the complaint arose, where the subject matter of the complaint is trivial, the complaint is frivolous, vexatious or not made in good faith or where the complainant does not have a sufficient personal interest in the subject matter of the complaint.

155 Privacy Act 1993, *op. cit.*, section 66(1)(b).

provide appropriate training for their staff. Even where the Commissioner finds that there has been an interference with privacy, settlement of the complaint is the preferred outcome.[156] Section 74 of the 1993 Act explicitly encourages the Commissioner to use his, "*best endeavours*," to settle the complaint, even without investigation, where it appears possible to do so.

The Commissioner also has the ability to **require the parties to attend what is known as a compulsory conference** with a view to achieving a resolution of the matter. Even where the Commissioner, as a result of his or her investigation, is of the opinion that the complaint has substance, he or she shall use his or her best endeavours to secure a settlement of the complaint and an assurance against repeat privacy-interfering behaviour by the agency concerned.[157] It is said that the **statutory emphasis is therefore on conciliation and dispute resolution**, rather than litigation. This is consistent with the educative thrust of the 1993 Act, allowing the complaints process to be used as a device for informing parties of their responsibilities and rights, and correcting the privacy-invasive practices of agencies in a non-punitive way.[158]

A further right of someone who considers that their privacy has been breached, is to refer their case for consideration by the **Human Rights Review Tribunal ("HRRT")**. The Commissioner may choose to do this where he is of the opinion that there has been an interference with privacy warranting referral to the Director of Human Rights Proceedings, but the complainant may also self-refer in certain circumstances: where the Commissioner finds that an interference with privacy has occurred but nonetheless decides not to refer the case to the Director; where the Director declines to pursue the case on behalf of the complainant or agrees that the complainant may bring proceedings; or where the Commissioner finds that no interference with privacy has occurred or has discontinued his or her investigation.[159]

If the **HRRT** finds on the balance of probabilities that an interference with the privacy of an individual has occurred, it has the **power to award various remedies**, including:[160]

- Declarations (that the action of a defendant is an interference with the privacy of an individual);
- Restraining orders (preventing the defendant from continuing or repeating the interference, or from engaging in, or causing or permitting others to engage in, conduct that constitutes an interference);
- Damages (up to a maximum of NZ$200,000);
- Orders specifying acts the defendant must perform in order to remedy the interference, or redressing any loss or damage suffered by the aggrieved individual; and
- Any other relief that the Tribunal thinks fit.

2.2. Proposed reforms

Under the proposed reforms, it should be noted that **no particular changes are being put forward to provide individuals with greater rights** insofar as the Information Privacy Principles are concerned. Instead, the focus of amendments to the existing legal framework are focused on measures enabling the identification, investigation and response to systemic privacy risks.

---

156 Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand*, *op. cit.*, p.64.

157 Privacy Act 1993, *op. cit.*, section 77.

158 Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand*, *op. cit.*, p.64.

159 Privacy Act 1983, *op. cit.*, section 83.

160 Privacy Act 1993, *op. cit.*, section 85(1).

With regard to the investigation and response to data protection breaches, **a proposed change to the complaints process** made by the Law Commission[161] has been endorsed by the Minister of Justice concerning "**access complaints**". This is a complaint by someone that he or she is unable to access his or her personal information retained by an agency.[162] Currently, if the Commissioner is unable to settle an access complaint, an enforceable decision can only be made by the HRRT; the Commissioner may only make recommendations. Tribunal proceedings are adversarial and court-like, and it is considered by the Minister of Justice that it is not an appropriate forum for resolving access complaints. It is therefore **proposed that the Commissioner be able to make enforceable decisions on access complaints** about what information should be released and which withheld. Under this proposal, the Commissioner would be able to issue an enforceable compliance notice, with such decision appealable before the HRRT.

3. Duties of the persons responsible for treatment

3.1. Current law

Under section 23 of the 1993 Act, **every agency[163] must ensure** that there are, within that agency, one or more individuals with the **role of *privacy officer***. The statutory duties of a privacy officer are:[164]

- the encouragement of compliance, by the agency, with the information privacy principles ("IPPs");
- dealing with requests made to the agency, in accordance with the 1993 Act;
- working with the Commissioner in relation to investigations into the agency; and
- otherwise ensuring compliance with the provisions of the Act.

There is no particular specified procedure or method under the 1993 Act to guide the privacy officer in this role. The officer has the discretion to devise programmes, training, standards, procedures and policies which are suitable to the particular agency.[165]

The **duties of an agency which handles personal information** are nevertheless defined by a number of the IPPs set out in Part 2 of the 1993 Act, or otherwise specified in codes of practice, where applicable. These can be summarised as follows:[166]

---

161 The Law Commission is an independent Crown Entity (see section 1 above for the meaning of this in relation to the OPC) whose role is to review the law of New Zealand and to make recommendations for law reform to the relevant Government Minister. See Law Commission website at http://www.lawcom.govt.nz/ (09.05.2016). Its report on reform of the 1993 Act is discussed in more detail in section 4 of this country report, below.

162 A right to access one's personal information is set out in Information Privacy Principle 6, featured in Part 2 of the Privacy Act 1993, *op. cit.*

163 For the meaning of Agency, see section 1 of this country report.

164 Privacy Act 1993, *op. cit.*, section 23.

165 Elizabeth Longworth & Tim McBride, *The Privacy Act – A Guide*, GP Publications 1994, Wellington, p. 280.

166 As summarised in Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand, op. cit.*, p.56-57.

IPP 1: Purpose of collection – personal information must not be collected unless the collection is for a lawful purpose and is necessary for that purpose.

IPP 2: Source of personal information – when information is collected, the collecting agency should make the individual aware that the information is being collected, the purpose for which it is being collected, who is collecting it and who will hold the information, the consequences of not providing the information, and that the individual has rights of access and correction.

IPP 3: Collection of information – when information is collected, the collecting agency should make the individual aware that the information is being collected, the purposes for which it is being collected, who is collecting it and who will hold the information, the consequences of not providing the information, and that the individual has rights of access and correction.

IPP 4: Manner of collection – personal information must not be collected by unlawful, unfair or unreasonably intrusive means.

IPP 5: Storage and security – agencies must safeguard against loss, misuse or unauthorised disclosure of personal information.

IPP 6: Access to personal information – individuals are entitled to confirmation of whether information is held about them, and to have access to it.

IPP 7: Correction – individuals are entitled to request correction of personal information and, if it is not corrected, to insist that a statement is attached to the information showing that a correction was sought.

IPP 8: Accuracy – agencies must take steps, before using or disclosing information, to ensure that it is accurate, complete, relevant, up-to-date and not misleading.

IPP 9: Retention only for as long as necessary – agencies should not keep personal information for longer than is necessary for the purpose for which it was collected.

IPP 10: Limits on use – personal information collected for one purpose should not generally be used for another purpose.

IPP 11: Limits on disclosure – personal information should not generally be disclosed except to the data subject or in connection with a purpose for which it was collected.

IPP 12: Unique identifiers – unique identifiers (such as IRD, bank customer, driver's licence or passport numbers) should be assigned only when necessary to enable an agency to operate efficiently. There can be no single identifier for use across all government agencies.

The obligations of an agency according to the IPPs were described by a Judge in a 2009 case as follows:

> *"In broad terms those principles require that personal information is not to be collected by any agency, unless the information is collected for a lawful purpose and is necessary for that purpose. An agency collecting personal information must generally seek to collect the information directly from the person concerned and make the individual aware of the fact the information is being collected, and for what purpose. The agency is required to keep the*

information secure, to give individuals access to it, and to allow individuals the right to request corrections to the information."[167]

Privacy Impact Assessments ("PIA"s) can be used by agencies to assess the impact of a project on personal data, and these are encouraged by the Privacy Commissioner. **PIAs are not a legislative requirement** apart from in certain cases, such as in relation to the collection and handling of biometric information under the Immigration Act 2009.[168] Instead, **guidance, in the form of a Privacy Impact Assessment Toolkit is issued by the OPC** for general use, on a voluntary basis, in both the public and private sector.[169] Part 1 allows agencies to determine whether they need to carry out a PIA at all, and Part 2 provides a step-by-step guide to doing a PIA.

It should be noted however that recent legislation in the form of the **Privacy Amendment Act 2013** also introduced amendments to the 1993 Act by implementing a new mechanism to allow the **sharing of personal information to facilitate the provision of public services** ("information-sharing" agreements). In certain circumstances, the lead Government agency is required to consult the Privacy Commissioner in relation to such a project with a view to addressing matters typically covered by a PIA, such as the uses to which a recipient agency may put the information, the safeguards to be adopted to ensure the security of the information shared and how general requirements of the Privacy Act relating to sharing programmes are to be met.[170]

3.2. Proposed reforms

Two important changes to the duties of agencies are included in the reforms proposed for the 1993 Act:

First, it is proposed that **agencies will be required to notify the Commissioner of certain breaches of data protection**. Currently, the Commissioner only becomes aware of privacy breaches through voluntary notification, complaints and media reports. The new regime will include **mandatory notification of breaches** enforced by compliance notices and enhanced penalties for non-compliance. This, it is said, will allow the Commissioner to better identify, investigate and address emerging privacy risks proportionately prior to harm occurring. The reforms propose a two-tier notification regime:[171]

- Tier one: agencies will have to take **reasonable steps to notify the Commissioner of any material breaches** as soon as reasonably practicable. In deciding if breaches are material,

---

167 *ANZ National Bank Ltd v Tower Insurance Ltd* 11/3/09, Judge Wylie, High Court Auckland CIV-2005-404-7271, [171] as cited in Steven Penk & Rosemary Tobin (eds.), *Privacy Law in New Zealand, op. cit.*, p.56.

168 Immigration Act 2009, section 32, available at http://www.legislation.govt.nz/act/public/2009/0051/latest/DLM1440630.html (18.04.2016).

169 Privacy Commissioner website, *Privacy Impact Assessment Toolkit*, 7th July 2015, available at https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/ (18.04.2016).

170 The Cabinet Manual (available at https://cabinetmanual.cabinetoffice.govt.nz/ (18.04.2016)) – which records the administrative and constitutional arrangements of executive government - requires government agencies to consult with the Privacy Commissioner when putting forward policy proposals or draft legislation that affects personal information. Part 9A of the Privacy Act (approved information-sharing agreements) and Part 10 (authorised information-matching programmes) specify when and how the Privacy Commissioner has to be consulted. "Information matching" refers to the comparison (whether manually or by means of any electronic or other device) of authorised information matching information with other personal information about for the purpose of producing or verifying information about an identifiable individual: Privacy Act 1993, *op. cit.*, section 97.

171 Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper, op. cit.*, paras 42-46.

agencies will take into account factors such as the sensitivity of the information, the number of people involved and whether there are indications of a systemic problem.

- Tier two: for more serious breaches, agencies will have to take **reasonable steps to notify the Commissioner and affected individuals of breaches** where there is a real risk of harm (such as actual or potential loss, injury, significant humiliation or adverse effects on rights or benefits).

Agencies that fail to notify the Commissioner of breaches will be liable, upon conviction, to a fine of up to $10,000. This only applies to private sector agencies. The Minister for Justice considers that the most effective deterrent for public sector agencies is 'naming and shaming'.

Secondly, it is proposed that there will be a **new Information Privacy Principle** to require New Zealand agencies to take reasonable steps to ensure that information disclosed overseas will be subject to **acceptable privacy standards in the foreign country**.[172] Cross-border disclosures occur when a New Zealand agency discloses information to an agency from a different country, for that agency's own use. At present, a disclosure is authorised if it is consistent with the purpose for which the information was obtained, the individual concerned authorises the disclosure or other exceptions apply. Once disclosed overseas, the information falls outside the 1993 Act's jurisdiction.

The new privacy principle will be accompanied by guidance about the definition of "acceptable privacy standards" and the steps agencies should take to meet the requirement that acceptable privacy standards are in place in the destination country. The **Commissioner will be able to publish a list of countries with acceptable privacy laws** in order that New Zealand agencies can determine relatively easily if overseas companies or organisations they are dealing with are likely to have adequate measures in place. Agencies will then not be liable for privacy breaches committed by the overseas agency in breach of any contractual measures or in reliance on foreign privacy laws, but will be liable where they have not taken reasonable steps to protect the information before it has left their control or if they have not confirmed that an exception to the principle applies.[173]

4. Big Data, Profiling, Internet of Things

It is widely considered that **technological developments** on the handling of personal information in different contexts have **not warranted specific amendments to the legal framework** or the 1993 Act itself. The flexibility offered by the Information Privacy Principles ("IPP"s) generally has the confidence of the Government, the Privacy Commissioner and the world of business.

As part of the ongoing review of the Privacy Act 1993, the **Law Commission undertook a consultation exercise**, asking, at the fourth and final stage of the review, if specific technologies, such as search engines and websites, social networking, cloud computing, deep packet inspection, location technologies, radio frequency identification and biometrics required any particular regulatory response, including legislative amendment. It reported that:

> *"Overall, submitters did not support any specific reforms to the Privacy Act to respond to technological developments, preferring guidance from the Privacy Commissioner and, where necessary, best practice rules and consideration if a code of practice.....The Privacy Commissioner's own submission suggested that what is important is that the Privacy Act is sufficiently flexible to respond appropriately to whatever new technologies arise now and in*

---

172 *Ibid*, paras 70-75.

173 New Zealand Government, *Privacy Act Review Q&A*, Beehive website, undated, available at https://www.beehive.govt.nz/sites/all/files/Privacy_Act_Reform_Q&A.pdf (20.04.2016), p.5.

the future, and that her Office has adequate powers to respond to new developments that pose threats to privacy."[174]

The Law Commission **concludes that changes in this regard are not needed to the 1993 Act itself**, and that on the whole, the privacy principles and that Privacy Commissioner's current functions and powers are adequate and sufficiently flexible to respond to the challenges posed by new technologies.[175]

In its 2014 proposal for the newly revised Privacy Act, the Office for the **Minister of Justice refers to the Law Commission's review**, acknowledging the technological advances that have been made in the 20 years since the 1993 Act was enacted. A single privacy breach, it recognizes, has the potential to cause large amounts of harm to a large number of individuals, rather than harm to a single individual. However, the problem, it says, is not that the legislation has failed to keep up with technological developments, but that there are **insufficient incentives for agencies to identify and address privacy risks** before breaches occur.[176]

The **broad regulatory framework based on the flexibility permitted by the IPPs will not therefore be reformed**. Rather than implementing prescriptive rules to address specific technological changes, the Minister for Justice agrees with the recommendations of the Law Commission to focus instead on **education and guidance for agencies**, coupled with reforms (as discussed above) designed to **reinforce the compliance framework** and to provide **more tools for the Privacy Officer** to identify, investigate and respond to systemic privacy risks.[177]

The grouping together, for example, of individual bundles of personal information for use by business to identify consumer trends and to assist targeted marketing is not prohibited by the current or revised privacy framework so long as such information remains anonymized and the individual that makes up part of that data set is not identifiable.[178] Where **Big Data analytics** of this kind are used for purposes that do identify the individual (by, for example, marketing directly to that person), **there must be compliance with the IPPs**. It may, for example, not be possible to use some information to market to the individual if he or she has not consented. Companies will typically get customers to provide consent as part of membership of loyalty schemes, permitting use of the data in this way.[179]

The Office of the Privacy Commissioner provides examples in its most recent Annual Report of how it is engaging in **initiatives designed to embrace the benefits of Big Data projects** particularly in the public sector. One such example is ***The Data Futures Partnership***,[180] established in August 2015. This is an independent cross-disciplinary group created by the New Zealand Government to develop innovative solutions to data-use issues. Its work is based on findings and insights of the *Data Futures Forum*, a committee of individuals from academia and the private and public sectors which has

---

174 Law Commission of New Zealand, *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4*, Report 123, June 2011, Wellington, available via https://privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform-resources/new-zealand-law-commission-privacy-review/ *(20.04.2016), para 10.57-10.59.*

175 *Ibid*, para. 10.6.

176 See Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper, op. cit.*, paras 24-40.

177 *Ibid.*

178 Peter Stubbs, *Digitalisation and Privacy Law*, internet article, 1 September 2014, available at http://blog.marketing.org.nz/2014/09/01/digitisation-privacy-law/ (20.04.2016).

179 International Comparative Legal Guides, contributed by Wigley & Company, *New Zealand, Data Protection 2015*, 13 May 2015, available at https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/new-zealand (20.04.2016), section 12.

180 Data Futures Partnership website, available at http://datafutures.co.nz/ (21.04.2016).

consulted widely with stakeholder groups, including business, government and non-government organisations to produce recommendations for the future of data sharing and data use in New Zealand. Like the 1993 Act, the consultation exercise **proposes a principles-based approach for safely managing and optimizing data use** in New Zealand and endorsed by the Privacy Commissioner. The **four guiding principles** are:[181]

1. *Value*: New Zealand should use data to drive economic and social value and create a competitive advantage.
2. *Inclusion*: All parts of New Zealand society should have the opportunity to benefit from data use.
3. *Trust*: Data management in New Zealand should build trust and confidence in our institutions.
4. *Control*: Individuals should have greater control over the use of their personal data.

In its submission to the consultation of the *Data Futures Forum*,[182] the **Office of the Privacy Commissioner supported this principles approach** and highlighted the role the 1993 Act plays in protecting the rights of individuals in 'big data' scenarios. It considers that the Privacy Act 1993, as it stands, already **provides New Zealand with a competitive advantage** for a number of reasons.

First, it considers that two key features of **New Zealand's privacy law** make it a **potential model for managing privacy**: (1) its definition of personal information is broad enough to encompass de-identified and pseudonymous information; (2) it provides broad exceptions to principles on collection, use and disclosure where information will be used in a form in which individuals will not be identified. If agencies have a lawful purpose for collecting personal information and do not intend to use it in a form in which individuals will be identified, it says, they can use and re-use it without having to obtain detailed consents that apply to all those future cases.[183] Secondly, the Commissioner claims that, "*one of the reasons the Privacy Act can effectively regulate the innovative use of personal information is because it has never been based on a legal concept of ownership.*" That the **1993 Act is not based on a model of ownership** means that the bundles of rights of individuals do not rely on establishing who might "own" information but instead focuses on who holds or controls the data, the rights of data subjects and the actions of agencies in those circumstances.[184]

In its submission, the Commissioner also refers to areas where steps could be taken to better support the four values set out by the *Forum*, including **two proposals which have particular relevance to Big Data**:[185]

It suggests, first, that the **Privacy Act should have stronger protections against re-identification of de-identified or pseudonymous data**. Consideration should be given, it says, to whether the Privacy Act should contain an explicit prohibition on re-identifying previously de-identified data in order to

---

181 New Zealand Data Futures Forum – Discussion Document 2, *Navigating the Data Future – Four Guiding Principles*, undated, available at https://www.nzdatafutures.org.nz/sites/default/files/NZDFF_Discussion%20document%202.pdf (21.04.2016), p.4.

182 Privacy Commissioner, *New Zealand's Data Future: A View From the Privacy Commissioner – Submission by the Privacy Commissioner to the New Zealand Data Futures Forum*, 4 July 2014, available at https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/New-Zealands-data-future-submission-by-the-Privacy-Commissioner.pdf (21.04.2016).

183 *Ibid*, p.3.

184 *Ibid*, p.4.

185 *Ibid*, pp. 5-6.

reassure people that they have means of redress if they suffer harm due to being successfully re-identified from supposedly anonymous data. Secondly, it says that the **Act could provide stronger rights to have information deleted**. Acknowledging that there is still a debate as to what a "**right to be forgotten**" actually requires, it states that the existing IPP 7, which provides the right to individuals to have information corrected, only applies to information that is inaccurate, out of date, incomplete or misleading, and that there may be situations where individuals might expect information to be deleted even where it is accurate.

It should be noted however, that **neither of these suggestions are featured in the policy paper setting out the basis for a revised draft Privacy Act**,[186] and therefore do not, at present, form part of the New Zealand Government's proposed reforms to existing legislation.

Similarly, the concept of the "***internet of things***", as another form of data sharing, is **not expressly recognized by existing legislation**, nor it is specifically targeted by proposed reforms. The idea of an *internet of things* and its significance for the future is recognized and discussed in government-commissioned research, such as that conducted by the New Zealand *Data Futures Forum*,[187] but it is **not, at present, suggested that legislative reform is required in order to address such phenomena**.

As with existing views about how to address the risks associated with Big Data, it may be inferred that the **principles-based approach** - including an emphasis on the harnessing of such personal information so long as it does not serve to identify particular individuals - may still be **relied on to address challenges presented by the *internet of things*.** One recent example, with which a parallel to the *internet of things* may be drawn, is **the use of "*smart meters*" by utility companies**. It was reported in February 2015, that the Privacy Commissioner had received enquiries from the public about such meters, increasingly being used by electricity companies.[188] These collect data at frequent intervals and communicate it directly to the electricity company. Finding that the data collected from such advanced meters potentially becomes personal information once it is associated with an account holder, power companies are, says the Privacy Commissioner, subject to the 1993 Act. This means they will need to ensure that the information is appropriately stored and handled and access to the information is restricted to the purposes for which it was collected. The Privacy Commissioner nevertheless states:

> *"While the introduction of smart appliances and how this will interact with advanced metering technology is speculative at present, we believe that it has the potential to make the information from smart meters more valuable. We are keeping a watching brief as the technology develops and may adjust our view as necessary in future."*[189]

---

186 See above, Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper, op. cit.*

187 See New Zealand *Data Futures Forum, New Zealand's Data Future – Full Discussion Paper*, undated, available at https://www.nzdatafutures.org.nz/sites/default/files/first-discussion-paper_0.pdf (25.04.2016), p.5.

188 See Privacy Commissioner, *Case Note 251185 [2015] NZ PrivCmr 3: Use of smart meters by utility companies*, 11 February 2015, available at https://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-251185-2015-nz-privcmr-3-use-of-smart-meters-by-utility-companies/ (25.04.2016).

189 *Ibid.*

5. Measures to promote privacy by design / privacy by default

The **only legislative measure with specific relevance to the impact of technological developments** on data protection is that listed among the functions of the Privacy Commissioner, as set out under section 13(1)(n) of the 1993 Act:

> *"to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring."*[190]

This is said to provide an opportunity for the Privacy Commissioner **to inform and raise awareness**, particularly in the public sector, *"as an initial step in encouraging Privacy by Design."*[191] This function to monitor technological developments is fulfilled in a number of ways, notably by: maintaining a technology section on the Office of the Privacy Commissioner's ("OPC") website; including a brief report on technology policy in the OPC's Annual Report; signalling technology issues and their impact on the work of the OPC in the "Statement of Intent";[192] including items on technological issues in the fortnightly newsletter, *Privacy News*;[193] making submissions on the legislation that mandates the use of particular technologies; and by reporting on specific projects undertaken by the OPC.[194]

As part of the consultation on reform of the 1993 Act, **the Law Commission asked whether express provision should be made in the Act for the privacy-enhancing technologies ("PETs")** which are typically incorporated into new information systems and information handling processes as part of the *Privacy by Design* approach. Following receipt of responses during the consultation exercise, the Law Commission concluded:

> *"PETs have an important role to play in ensuring that the standards embodied in the privacy principles are observed in a wide range of personal information handling contexts. However, we think that it would run counter to the flexibility of the privacy principles and their technological neutrality for the Act to specify that any particular measures must be taken. It may also be counterproductive to mandate that certain PETs must be used, given the rapid rate of technological development."*

It is therefore anticipated that **this educational approach to PETs and their incorporation into *privacy by design* models will continue to be pursued** under the Privacy Commissioner's existing functions. This will involve, as is presently the case, raising awareness of the role of PETs, when such technologies can be adopted by agencies in personal information handling and advice to consumers on how to protect their personal information in these circumstances. This approach is consistent with those promoted in Australia and the UK.

---

190 Privacy Act 1993, *op. cit.*, section 13(1)(n).

191 According to Law Commission of New Zealand, *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4, op. cit.*, p. 253.

192 The OPC's *Statement of Intent* sets out the intentions and undertakings of the OPC over a 5 year period. The current *Statement of Intent* is available at https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/SOI-Office-of-the-Privacy-Commissioner-2014-18-FINAL.pdf (04.05.2016).

193 Officer of the Privacy Commissioner, *Privacy News*, available at https://www.privacy.org.nz/news-and-publications/privacy-news/ (04.05.2016).

194 Law Commission of New Zealand, *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4, op. cit.*, p. 253.

The **Law Commission did not make any specific recommendations in relation to PETs**, but did recommend that the Privacy Commissioner consider convening an **expert privacy by design panel** made up of experts with the aim of promoting best practice, particularly within the public sector.[195] Such a panel, it said may be an efficient way to promote PETs without placing an additional resource burden solely on the OPC. ***This recommendation was accepted by the Office of the Minister of Justice***, and is noted as having been transferred to the OPC for consideration.[196] No further information on the implementation of this recommendation has been made available.

6. Data portability

There are **no specific legislative or other provisions aimed at portability of data**, nor is there any right, under New Zealand law, to take one's own data elsewhere.

Similarly, there are also, as yet, **no provisions for recognising a *right to be forgotten***. One of the Assistant Data Protection Commissioners, Joy Liddicoat, points out however, that there are a number of other **existing mechanisms** that, put together, provide a strong basis for ensuring personal **information can nevertheless be removed or corrected**. As well as Principles 7 and 8 of the IPPs, which place a continuing obligation on agencies to ensure that data is accurate, up to date, complete relevant and not misleading (and which afford individuals the right to request correction of incorrect personal information), she refers to the wide range of legislative and common law measures which may be relied on to secure the deletion of personal data.[197]

Recent commentary from the **Office of the Privacy Commissioner** nevertheless acknowledges the inadequacy of deletion of information as the only remedy available to an individual – particularly where he or she is dissatisfied, for example, with one online provider who manages his or her personal data. In an article[198] published at the beginning of 2016, another Assistant Data Protection Commissioner, Blair Stewart, lists **data portability** as one of a number of new principles recognised in other countries that has **not yet been directly taken into account in the ongoing proposed reforms** for the 1993 Act:

The Office of the Privacy Commissioner has confirmed to us that current discussions on this topic are **internal** only, and have not been shared with the Ministry of Justice.[199]

---

195 Law Commission of New Zealand, *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4, op. cit.*, p. 254.

196 Office of the Minister of Justice, *Reforming the Privacy Act 1993 – Policy Paper, op. cit.*, Appendix 1, Part A, item 103.

197 Taken from Joy Liddicoat, *The right to be forgotten*, Office of the Privacy Commissioner, Wellington, 7th May 2015, available at https://www.privacy.org.nz/assets/Files/Speeches-presentations/Right-to-be-Forgotten-Joy-Liddicoat.pdf (09.05.2016), p. 7. For more information on these measures, see section 2 of this country report, above.

198 Blair Stewart, *Privacy proposals for the digital age*, website of the Privacy Commissioner of New Zealand, 14 January 2016, available at https://www.privacy.org.nz/blog/privacy-proposals-for-the-digital-age/ (04.05.2016).

199 As per email of 6th May 2016 from Tim Henwood, Senior Policy Adviser (Technology), Office of the Privacy Commissioner to John Curran, Juriste, Swiss Institute of Comparative Law.

E. SINGAPUR[200]

Einführung

In Singapur wurde 2012 ein Datenschutzgesetz erlassen (Personal Data Protection Act «PDPA»), dessen verschiedene Teile vom Januar 2013 bis Juli 2014 gestaffelt in Kraft getreten sind. Die Notwendigkeit eines Datenschutzgesetzes wurde auch mit den Ambitionen Singapurs als «High Tech» Zentrum begründet.[201] Der Schutz der Privatsphäre als Grundrecht steht also weniger im Zentrum als in anderen Staaten. Entsprechend ist das Gesetz in erster Linie auf private Unternehmen anwendbar, aber insbesondere nicht auf den öffentlichen Sektor[202], und es scheint unklar, welche Regeln dort gelten, da die diesbezüglichen Richtlinien nicht öffentlich sind.[203] Die Vorschriften zur Bearbeitung von persönlichen Daten sind im Übrigen auch nicht auf Einzelpersonen anwendbar, sofern sie privat oder persönlich oder aber im Rahmen ihrer Anstellung handelt.[204]

Neben den allgemeinen materiellen Datenschutzbestimmungen sowie denjenigen zur Aufsichtsbehörde, zu Verfahren und Durchsetzung enthält der Personal Data Protection Act ausführliche Bestimmungen über das «Do Not Call Registry». Es handelt sich um Listen von Telefonnummern, an welche keine Werbenachrichten gesendet werden dürfen. Jede Person mit einer Telefonnummer kann sich auf diese Liste setzen oder sich von ihr entfernen lassen.[205]

1. Aufsichtsbehörde

Die mit dem Datenschutzgesetz geschaffene Behörde, die Datenschutzkommission (*Personal Data Protection Commission*), hat als Hauptaufgabe, das Gesetz auszuführen und durchzusetzen.[206] Daneben hat sie verschiedene unterstützende Funktionen wie z.B. die Beratung der Regierung, die Sensibilisierung der Bevölkerung, das Durchführen von Forschung und Veranstaltungen, beratende Dienstleistungen allgemein, ist aber auch für technische Kooperation und internationalen Austausch zuständig.[207] Im Rahmen dieser Funktionen kann die Kommission Richtlinien verfassen, welche ihre Auslegung der Gesetzgebung ausführen.[208] Diese Richtlinien sind allerdings nicht rechtlich bindend[209] und werden deshalb als *Advisory Guidelines* bezeichnet. Schliesslich hat die Kommission ebenfalls relativ weitgehende Untersuchungsbefugnisse (s. unten).[210]

Das Gesetz sieht einen breiten Rahmen (3 bis 17 Mitglieder) für die Kommissionsgrösse vor; aktuell besteht die Kommission aus **5 Mitgliedern**.[211] Es handelt sich dabei überwiegend um Angehörige der

---

200 Dieser Bericht beruht auf den am Schweizerischen Institut für Rechtsvergleichung sowie online vorwiegend in englischer Sprache verfügbaren Informationen, wurde aber nicht von einer im Recht vom Singapore ausgebildeten Person verfasst.

201 S. S. Chesterman, Date Protection Law in Singapore. Privacy and Sovereignty in an Interconnected World, Singapur 2014, S. xii, mit Verweis auf Minister Yaacob Ibrahim.

202 Section 4 (1) (c) PDPA.

203 Chesterman, zit., S. xiii.

204 Section 4 (1) (a) und (b) PDPA.

205 Teil IX PDPA.

206 Section 6 (g) PDPA.

207 Section 6 (a) bis (f) PDPA.

208 Sectinon 49 PDPA.

209 So ausdrücklich in Introduction to the Guidelines, S. 5.

210 SEction 50 PDPA, s. dazu unten.

211 Section 5 (1) PDPA ; zu den aktuellen Mitgliedern s. die Website der PDPC: www.pdpc.gov.sg (Commission Members).

Telekommunikationsbehörde «Infocomm Development Authority of Singapore (IDA)». Die Mitglieder werden vom Kommunikationsminister ernannt. Das Gesetz sieht keine Unabhängigkeit der Behörde vor, und die Finanzierung scheint derjenigen anderer öffentlicher Behörden zu entsprechen.

Neben der Kommission kann der Minister ein **beratendes Komitee** ernennen, welches die Kommission in Bezug auf deren Funktionen berät.[212] Das beratende Komitee umfasst momentan 12 Personen aus Verwaltung, Wissenschaft und Praxis.[213] Zudem kann der Minister einen **Verwaltungsapparat** (Administration Body) einsetzen, der Budget erstellt und die Buchhaltung führt, Berichterstattungspflichten für die Kommission wahrnimmt, diese verwaltungsmässig auch in anderer Hinsicht unterstützt und die Kommission auch in Zivilverfahren vertreten kann.[214]

Die Kommission selbst kann selbst **Inspektoren** einsetzen und diesen Aufgaben und Kompetenzen delegieren.[215] Die Inspektoren werden in der Regel die **Aufsichtsfunktionen** der Kommission wahrnehmen. Die Aufsichtsfunktion beinhaltet einerseits das Behandeln von Individualbeschwerden im Zusammenhang mit Zugangs- oder Änderungsersuchen, andererseits kann die Kommission auch ohne Vorliegen einer Beschwerde Untersuchungen durchführen und den betroffenen Unternehmen Anweisungen im Zusammenhang mit deren Bearbeitung geben.[216] Dies beinhaltet auch eine Aussprache von Bussgeldern bis zu § 1 Million (ca. CHF 700'000.--). Die Anweisungen der Kommission sind dabei gerichtlich durchsetzbar,[217] können aber auch vor einer Rekursinstanz, dem *Appeal Panel*, und danach vor Gerichtsinstanzen angefochten werden.[218]

Die Kommission und die Inspektoren haben relativ weitgehende **Untersuchungsbefugnisse**. Diese sind in einem Anhang zum Gesetz geregelt und umfassen ein Recht auf Informationserteilung und Dokumentenherausgabe, ein Zutrittsrecht auf Privatgrundstücke mit vorgängiger gerichtliche Ermächtigung oder ohne (aber nach schriftlicher Ankündigung) und ein Recht auf Beschlagnahmung von Dokumenten und Informationen.[219]

2. Rechte der Betroffenen

Betroffene haben gegenüber datenverarbeitenden Unternehmen ein **Recht auf Zugang** zu den persönlichen Daten, welche dieses Unternehmen hat, sowie auf Information, wie diese Daten im Jahr vor dem Gesuch verwendet oder bekannt gegeben wurden.[220] Ausgenommen sind eine Reihe von Daten, insbesondere im Zusammenhang mit Examen bei einer Bildungsinstitution oder mit Schiedsgerichten und Mediationszentren sowie Information im Zusammenhang mit einer Strafverfolgung, Daten über Meinungen welche zur Evaluation aufbewahrt werden, oder sofern der Aufwand zur Gewährung von Zugang unverhältnismässig wäre.[221] Kein Zugangsrecht besteht u.a. auch bei einem Gefährdungsrisiko für die Gesundheit oder Sicherheit der betreffenden Person oder von Drittpersonen oder falls die Information Angaben über Drittpersonen beinhalten würde.[222]

---

212 Section 7 PDPA.

213 S. die Internetseite der Personal Data Protection Commission, https://www.pdpc.gov.sg/about-us/advisory-committee.

214 Section 9 PDPA.

215 Section 8 PDPA.

216 Section 28, 29 und 50 PDPA.

217 Section 30 PDPA.

218 Section 33 ff. PDPA.

219 Ausführlich : Schedule 9 zum PDPA.

220 Section 21 (1) PDPA.

221 5. Anhang zum PDPA

222 Section 21 (3) PDPA.

Betroffene Personen haben auch ein Recht, die **Korrektur** oder Ergänzung von Daten zu verlangen, welche sich unter der Kontrolle eines Unternehmens befinden.[223] Dies bewirkt grundsätzlich auch eine Korrektur bei den Organisationen, welche die Information vom betroffenen Unternehmen innerhalb eines Jahres vor Antrag auf Korrektur erhalten haben.[224] Auch hier bestehen Ausnahmen, insbesondere im Zusammenhang mit Bildungsinstitutionen und Schiedsgerichtsverfahren, sowie zur Änderung von Meinungsäusserungen, wobei diese weniger zahlreich sind als beim Recht auf Zugang.[225]

Wie bereits erwähnt (1.) können betroffene Personen an die *Data Protection Commission* gelangen, wenn ein Unternehmen ihrem Antrag nicht entspricht oder dafür (zu hohe) Gebühren verlangt. Die Kommission kann entsprechende **Beschwerden** direkt behandeln oder mit Zustimmung beider Parteien einer **Mediation** zuführen.[226] Die entsprechenden Verfahren werden in der Regel durch die Konsumentenschutzvereinigung Singapur (*Consumer Association Singapore* – CASE) oder das *Singapore Mediation Center* durchgeführt.[227] Schliesslich kann jede Person, welche durch eine Verletzung seiner Rechte oder der Grundprinzipien des Datenschutzrechts (inkl. des Zustimmungsprinzips, s. dazu unten, 3.) einen Schaden erlitten hat, ein **Zivilverfahren** anstreben, ausser ein Verfahren vor der Kommission ist noch im Gang.[228]

Weitere Rechte ergeben sich aus Pflichten der für die Datenbearbeitung verantwortlichen Person, so z.B. das Recht, über den Zweck einer Datenbearbeitung[229] und richtig über die Datenbearbeitung als solche sowie über eine Kontaktperson für allfällige Fragen[230] **informiert** zu werden,[231] oder aber das Recht, Dienstleistungen oder Produkte zu beanspruchen **ohne dafür mehr persönliche Daten preis geben zu müssen**, als für diese Dienstleistung oder dieses Produkt vernünftigerweise angebracht ist.[232] Die betroffene Person kann auch jederzeit die **Zustimmung** zu einer Datenbearbeitung **zurück ziehen**.[233]

3. Pflichten der datenbearbeitenden Organisation

Wie in der Einführung erwähnt regelt der PDPA in erster Linie Pflichten der Organisationen, welche Daten bearbeiten. Die Datenschutzkommission führt in einer allgemeinen Einführung zu den Richtlinien der Datenschutzkommission (s. dazu 1.) zusammenfassend aus, dass datenbearbeitende Organisationen neun Pflichten haben: die Pflicht zum Einholen der Zustimmung (*consent obligation*), die Pflicht zur Datenbearbeitung innerhalb eines bestimmten Zwecks (*purpose limitation obligation*), die Pflicht zur Mitteilung des Zwecks (*notification obligation*), die Pflicht zur Gewährung von Zugang und Vornahme von Korrekturen (*access and correction obligation*), die Pflicht zur Genauigkeit der Daten (*accuracy obligation*), die Pflicht zum Schutz der Daten (*protection obligation*), die Pflicht zur

---

223 Section 22 (1) PDPA.

224 Section 22 (2) und (3) PDPA : ein Weiterleiten ist nicht notwendig, wenn das Unternehmen vernünftige Gründe hat, die Information nicht zu korrigieren, oder wenn die beantragende Person zustimmt.

225 Section 22 (6) und (7) sowie Anhang 7 zum PDPA.

226 Section 27 PDPA.

227 Gemäss der Website der Kommission wurde mit diesen zwei Organisationen entsprechende Vereinbarungen geschlossen, s. https://www.pdpc.gov.sg/legislation-and-guidelines/mediation.

228 Section 32 PDPA.

229 Section 20 PDPA.

230 Section 20 (1) (c) PDPA.

231 Section 14 (2) (b) PDPA.

232 Section 14 (2) (a) PDPA : die Bestimmung verbietet es Organisationen, die Zustimmung zur Bearbeitung von persönlichen Daten, die über das Angebrachte («reasonable») hinausgeht, als Voraussetzung einer Dienstleistung oder eines Produkts zu machen.

233 Section 16 PDPA.

zeitlich begrenzten Datenbearbeitung (*retention obligation*), die Pflicht, Daten nicht ohne entsprechende Vorkehrungen ins Ausland zu übermitteln (*transfer limitation obligation*) sowie die Pflicht, Verfahren und Grundsätze zur Einhaltung der Datenschutzgesetzgebung zu treffen (*openness obligation*).[234] Diese Pflichten werden im Folgenden etwas genauer ausgeführt.

Im Rahmen der Grundregeln (3. Teil des Gesetzes) muss die Organisation **eine oder mehrere natürliche Personen** bezeichnen, welche für die Einhaltung der Datenschutzbestimmungen zuständig ist.[235] Die **Kontaktinformationen** für mindestens eine betreffende Person müssen veröffentlicht werden.[236] Zudem müssen Organisationen **Verfahren und Richtlinien** entwickeln, welche die Einhaltung der Datenschutzgesetzgebung sowie die Behandlung von Beschwerden ermöglichen, und diese auf Anfrage Drittpersonen mitteilen.[237] Die Advisory Guidelines der Kommission sprechen in diesem Zusammenhang von einer Pflicht zur Offenheit (*openness obligation*).[238]

Entsprechend einem Grundprinzip des PDPA hat jede datenbearbeitende Organisation die Pflicht, vor einer Datenbearbeitung die **Zustimmung** der betroffenen Person einzuholen, es sei denn, dies sei gemäss Gesetz nicht nötig (*consent obligation*).[239] Das Gesetz enthält in der Tat eine Vielzahl von Ausnahmen, wobei für die Erhebung (*collection*) und die Benutzung (*use*) sowie die Weitergabe (*disclosure*) verschiedene Listen bestehen (z.B. die klar im Interesse der betroffenen Person stehende Datenerhebung, sofern das Einverständnis nicht rechtzeitig erteilt werden kann; Erhebung von öffentlich verfügbaren Daten; Datenbearbeitung im nationalen Interesse; Datenerhebung zum Zweck der Evaluation von Kandidaten für ein Arbeitsverhältnis, im Bildungsbereich, im sportlichen und künstlerischen Bereich sowie zur Erteilung von Sozialhilfe oder von öffentlichen Gesundheitsdienstleistungen; Datenerhebung zu künstlerischen Zwecken; Datenbearbeitung zum Eintreiben von Schulden oder im Rahmen von Krediten; Datenbearbeitung, die im Rahmen eines Arbeitsverhältnisses notwendig ist; Datenerhebung für die Berichterstattung).[240] Zudem besteht eine Zustimmungsfiktion, wenn die betroffene Person freiwillig (*voluntarily*) eigene Daten mitteilt und davon ausgegangen werden kann, dass dies vernünftigerweise (*it is reasonable*) so geschieht.[241] Das Zustimmungserfordernis scheint also weniger weit zu gehen als in anderen Rechtsordnungen.

Eine gültige Zustimmung setzt u.a. voraus, dass die betroffene Person im Voraus korrekt über den **Zweck** der Datenbearbeitung **informiert** hat.[242] Die Datenbearbeitung darf nur für diese Zwecke erfolgen, und auch dann nur, wenn die Zwecke «vernünftig» sind (*purpose limitation obligation*).[243]

Die datenbearbeitende Organisation muss ebenfalls allen vernünftigen Aufwand betreiben, um die **Korrektheit und Vollständigkeit der Daten** sicherzustellen, sofern diese für einen die betroffene Person angehenden Entscheid verwendet wird oder möglicherweise einer andere Organisation weitergegeben wird.[244] Die datenbearbeitende Organisation hat ebenfalls eine **Sicherungspflicht**. Sie

---

234 Introduction to the Guidelines, verfügbar unter https://www.pdpc.gov.sg/docs/default-source/introduction-to-the-advisory-guidelines/introduction-to-the-guidelines.pdf?sfvrsn=0, S. 2-3.

235 Section 11 (3) PDPA.

236 Section 11 (5) PDPA.

237 Section 12 PDPA, s. dazu insbesondere

238 Kapitel 20 der Advisory Guidelines on Key Concepts in the PDPA, verfügbar unter https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines/key-concepts---chapter-20-%28150716%29.pdf?sfvrsn=2.

239 Section 13 PDPA.

240 Schedule 2 zum PDPA.

241 Section 15 PDPA.

242 Section 14 PDPA.

243 Section 18 (a) PDPA.

244 Section 23 PDPA.

muss Massnahmen ergreifen, um unerlaubten Zugang und Eingriff in die Daten zu verhindern.[245] Für die Sicherung von in elektronischen Medien gespeicherten persönlichen Daten hat die Datenschutzkommission eine Anleitung publiziert, welche « good practices» beispielhaft aufzählt.[246]

Schliesslich besteht eine Pflicht zur **Zerstörung oder Anonymisierung** der Daten, sobald das Behalten der Daten nicht mehr dem Zweck entspricht und kein rechtlicher oder wirtschaftlicher Grund (*business purpose*) für die Erhaltung der Daten besteht.[247]

Die **Weitergabe von Daten** in ausländische Rechtsordnungen ist grundsätzlich nur möglich, wenn sichergestellt wird, dass die datenempfangende Organisation im Ausland ähnlichen rechtlichen verbindlichen Standards unterworfen ist wie die in Singapur.[248]i Die Kommission kann allerdings Organisationen auf deren vom grundsätzlichen Verbot ausnehmen.

Die Pflichten sind mit ausführlichen **Straf- und Haftungsbestimmungen** versehen, wobei im Grundsatz die Organisation und kaum die Einzelpersonen haften[249]

4. Big Data, Profiling, Internet of Things

Der PDPA enthält keine Bestimmungen zu Big Data, Profiling oder Internet of Things. Die Kommission nimmt aber in Richtlinien mindestens indirekt auf gewisse Aspekte Bezug, welche insbesondere im Zusammenhang mit Big Data und Profiling von Bedeutung sind. So enthalten die *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*[250] eingehende Ausführungen über Anonymisierung sowie über die Aktivitäten auf Internet.[251]

Das Kapitel zur Anonymisierung ist auf Big Data ausgerichtet. Dabei wird ausgeführt, dass die Anonymisierung von Daten es ermögliche, Forschung und «data mining» durchzuführen, auch wenn

---

245 Section 24 PDPA. In Kapitel 17 der *Advisory Guidelines on Key Concepts in the PDPA* (vom 16.07.2016) wird ausgeführt, dass im Einzelfall geeignete Lösungen gefunden werden müssen, wobei in der Regel technische, regulatorische und personelle Massnahmen getroffen werden sollten (insbesondere N 17.3), vefügbar unter https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines/key-concepts---chapter-17-%28150716%29.pdf?sfvrsn=2.

246 Guide to Securing Personal Data in Electronic Medium vom 08.05.2015, revidiert am 20.07.2016, verfügbar unter https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-securing-personal-data-in-electronic-medium-v2-0-%28200716%29.pdf?sfvrsn=2.

247 Section 25 PDPA.

248 Section 26 (1) PDPA verbietet die Weitergabe ausserhalb des Territoriums « ausser in Übereinstimmung mit Anforderungen in diesem Gesetz zur Sicherstellung eines Datenschutzstandards, der mit demjenigen in Singapore vergleichbar ist» (An organisation shall not transfer any personal data to a country or territory outside Singpore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of proteciton to personal data so transferred that is comparable tot he protection under this Act.) Da abgesehen von der Ausnahmebestimmung (section 26 (2) PDPA) keine weitere Bestimmung diesbezüglich besteht, ergibt sich die Tragweite nicht aus dem Gesetz. Die Ausführungsbestimmungen sehen vor, dass überprüft werden muss, ob die Organisation im Ausland ähnlichen Standards unterworfen ist, ausser es liegt eine Zustimmung mit der Datenübertragung ins Ausland vor.

249 Section 51 ff. PDPA und section 60 PDPA.

250 Vom 24.09.2013, revidiert am 09.06.2016, verfügbar auf der Internetseite der Kommission unter https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/main-advisory-guidelines#AG2.

251 Kapitel 3 und 7.

diesbezüglich keine Zustimmung vorliege.[252] Im Anschluss daran werden verschiedene Anonymisierungstechniken erwähnt (3.8), es wird aber auch auf Grenzen und Schwierigkeiten hingewiesen, beispielsweise dass die Verfügbarkeit anderer Daten die Tiefe der Anonymisierung bestimme, dass eine Anonymisierung einem allfälligen Profiling-Zweck entgegenstehen kann (Ziff. 3.10 bis 3.11). Sehr ausführlich wird danach das Risiko der Wieder-identifizierung behandelt, welches insbesondere bei einer Weitergabe oder Veröffentlichung berücksichtigt werden müsse (3.13 ff.). Dabei werden Massnahmen beschrieben, welche das entsprechende Risiko vermindern können (3.21 ff. und 3.30 ff). Im Grundsatz führt die Kommission aus, dass nur (aber immerhin) bei einem hohen Risiko der Wieder-Identifizierung die Daten als persönliche Daten qualifiziert werden und der PDPA anwendbar ist (Ziff. 3.28). Es wird empfohlen, dass Unternehmen das entsprechende Risiko testen (3.41 ff.). Im ganzen Kapitel wird wiederholt auf Code of Practice des Information Commissioner's Office im Vereinigten Königreich hingewiesen. Die Ausführungen sollen also gewisse Rechtssicherheit schaffen und die Big Data Verarbeitung damit erleichtern.

Die Thematik der Big Data wird auch durch andere, **nicht normative Massnahmen** angegangen. So wurden datenschutzrechtliche Herausforderungen des Big Data z.B. im Rahmen von Veranstaltungen behandelt.[253] Dies gilt auch für das *Internet of Things,* das insbesondere in öffentlichen Ansprachen von Mitgliedern der Kommission erwähnt wird.[254]

5. Massnahmen zur Förderung von Privacy by Design / by Default

Der PDPA sieht keine spezifischen Massnahmen zur Förderung der Privacy by Design / by Default vor. Auch in den Richtlinien lässt sich kein entsprechender Ansatz erkennen. Allerdings werden sehr oft die Begriffe «notwendig» und «vernünftig» verwendet, welche eine entsprechende Förderung zulassen würden, aber nicht notwendig bedingen.[255] Ein Anzeichen einer Förderung der Wirtschaft beim Verfolgen von «privacy by design» ist eine von der Datenschutzkommission veröffentlichter Werbeartikel darüber, dass Master Card den *Privacy by Design* Ansatz verfolgt und damit gute Erfahrungen macht.[256]

---

252 Ziff. 3.5 der Advisory Guidelines on the Personal Data Protection Act for SElected Topics, zit.

253 So das von der Kommission organisierte 4. Datenschutzseminar vom 20.07.2016, s. dazu die Ausführungen des Kommunikations- und informationsministers Yacoob Ibrahim, verfügbar unter https://www.mci.gov.sg/web/corp/press-room/categories/speeches/content/opening-of-the-fourth-personal-data-protection-seminar.

254 Z.B. die Angaben des Vorsitzenden der Kommission anlässlich der Publikation der neuen Richtlinien, zitiert im Media Release der Kommission vom 20. Juli 2016, verfügbar unter https://www.pdpc.gov.sg/docs/default-source/media/seminar-2016-pr/media-release---organisations-can-better-protect-pd-%28200716%29.pdf?sfvrsn=2; s. auch die in der folgenden Fussnote erwähnten Ausführungen des Vorstehers der Kommission vom 25.04.2016.

255 S. dazu die Ausführungen des Vorstehers der Kommission, Leon Kheng Thai, anlässlich der 6. Europäischen Datenschutzkonferenz vom 25.04.2016 in Berlin, der die Unbestimmtheit als Vorteil im Rahmen einer möglichen Nutzung von Daten für Big Data und Internet of Things erwähnt (verfügbar unter https://www.pdpc.gov.sg/news/press-room/page/0/year/All/keynote-speech-by-mr-leong-keng-thai-chairman-of-pdpc-at-the-6th-european-data-protection-days-conference-monday-25-april-2016-in-berlin-germany).

256 Privacy by design, verfügbar unter https://www.pdpc.gov.sg/docs/default-source/PDPC-Ads/pdpc-newspaper-ad---mastercard.pdf?sfvrsn=2.

6. Datenportabilität

Der PDPA enthält keine Bestimmung zur Datenportabilität, und es sind keine weiteren Massnahmen diesbezüglich ersichtlich.

F. USA

Overview

There is no single, comprehensive federal law regulating the collection and use of personal date; U.S. law in this area is a patchwork of federal and state statutes, regulations and case law which not only overlap but may contradict each other.[257]

What follows are a few examples of what law exists on the subject in the U.S. as well as an update of our prior opinion on California.

1. Federal Law

The notion of a "right to privacy" with respect to marriage, intimate relations and reproductive rights is essentially a U.S. Supreme Court extension ("penumbral rights"[258]) of the First Amendment.[259]

Most restrictions on the collection and introduction into evidence by the government of data in the criminal context comes from the case-law based on the 4th Amendment[260].

There is also a wide range of federal legislation on various aspects of privacy rights, many of which (more than 70[261]) are enforced by the Federal Trade Commission (FTC)[262], such as

- the Children's Online Privacy Protection Act (COPPA)[263],
- the Fair Credit Reporting Act[264] and the Controlling the Assault of Non-solicited Pornography and Marketing Act known as the CAN-SPAM Act[265] for consumer protection

---

257 Jolly, I, *Data Protection in the United States: Overview,* Prac. L. (July 1, 2014), http://us.practicallaw.com/6-502-0467.

258 *See, e.g. Griswold v. Connecticut*, 381 U.S. 479 (1965), *Roe v. Wade*, 410 U.S. 558 (2003), *Planned Parenthood v. Casey*, 505 U.S. 833 (1992), Obergefell v. Hodges, 576 U.S. ___ (2015).

259 Amendment I, U.S. Constitution which provides as follows :
The First Amendment guarantees freedoms concerning religion, expression, assembly, and the right to petition. It forbids Congress from both promoting one religion over others and also restricting an individual's religious practices. It guarantees freedom of expression by prohibiting Congress from restricting the press or the rights of individuals to speak freely. It also guarantees the right of citizens to assemble peaceably and to petition their government.

260 Amendment IV, U. S. Constitution which provides as follows :
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

261 *See* Statutes Enforced by the Federal Trade Commission available at https://www.ftc.gov/enforcement/statutes.

262 *See* the website of the FTC at: https://www.ftc.gov/about-ftc.

263 15. U.S.C. §§ 6501-6505.

264 15 U.S.C. § 1681.

265 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.

- various sections of the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act[266] and the Dodd-Frank Act Wall Street Reform and Consumer Protection Act[267] concerning financial information, or
- concerning health information privacy, the Health Insurance Portability and Accountability Act (HIPAA)[268], enforced by the Department of Health and Human Services[269] and,
- in the criminal context, the Electronic Communications Privacy Act[270] and the Computer Fraud and Abuse Act[271].

Although not law, in itself, the Consumer Privacy Bill of Rights was released by the White House in 2012.

2. California

The following is a summary of modifications to the law of the State of California made since January 1, 2015.

Authorities:
The California Office of Information Security is now part of the California Technology Agency and is located at this address http://www.cio.ca.gov/OIS/
The California Office of Privacy Protection was defunded and is now part of the State and Consumer Services Agency (SCSA), located at this address http://www.privacy.ca.gov

Legislation:
California Legislation has been amended to include, *inter alia,* the following:

- A definition of the term "hosting platform".[272]
- The obligation for any business that owns or licenses certain data to notify any person whose data may have been acquired by an unauthorized person as a result of any breach of security of their system[273]
- Specific obligations of notice and disclosure of California State universities concerning alumni.[274]

---

266 Pub. L. 106-102 codified in relevant part at 15 U.S.C. §§ 6801-6809 and §§ 6821-6827.

267 Pub. L. 11-203.§

268 Public Law 104-191, codified in scattered sections of title 42 U.S. Code.

269 See http://www.hhs.gov/hipaa/.

270 18 U.S.C. § 2510 *et seq.*

271 18 U.S.C. §1030.

272 West's Ann.Cal.Bus. & Prof.Code § 22590 "Hosting platform" defined:
As used in this chapter, a "hosting platform" means a marketplace that is created for the primary purpose of facilitating the rental of a residential unit offered for occupancy for tourist or transient use for compensation to the offeror of that unit, and the operator of the hosting platform derives revenues, including booking fees or advertising revenues, from providing or maintaining that marketplace. "Facilitating" includes, but is not limited to, the act of allowing the offeror of the residential unit to offer or advertise the residential unit on the Internet Web site provided or maintained by the operator.

273 West's Ann.Cal.Civ.Code § 1798.82 available at:
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82 (Feb. 4, 2016). See, also: West's Ann.Cal.Civ.Code § 1798.29, available at:
http://www.leginfo.ca.gov/.html/civ_table_of_contents.html (Feb. 4, 2016).

274 West's Ann.Cal.Educ.Code § 92630 available at:
http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=edc (Feb. 4, 2016).

- A Student Online Personal Information Protection Act[275]
- A provision of the Education Code providing that the posting of a "burn page" is grounds for expulsion.[276]
- The Consumer Legal Remedies Act.[277]
- Regulations concerning Automated license plate recognition ("ALPR") procedures and practices[278]
- Section of the Penal Code criminalizing unauthorized access to computers, computer systems and computer data[279]
- Modifications made to California's Anti-SLAPP[280] motion (in cases of libel and slander on the Internet)[281] An anti-SLAPP motion allows a defendant to file a special motion to strike a complaint filed against him or her based on an "act in furtherance of [such person's] right of petition or free speech under the United States or California Constitution in connection with a public issue" early in the proceedings and, where the motion is successful, to obtain costs and attorney's fees (as opposed to the ordinary "American Rule" pursuant to which each party bears his or her own such costs and fees.

---

275 See: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177 (Feb. 4, 2016).

276 West's Ann.Cal.Educ.Code § 48900, available at: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=48001-49000&file=48900-48927 (Feb. 4, 2016).

277 A new section of West's Ann.Cal.Civ.Code § 1770.

278 West's Ann.Cal.Civ. § 1798.90.51-53.

279 West's Ann.Cal.Penal Code § 502, available at: http://support.piercecollege.edu/1521a/References/California%20Penal%20Code%20Computer%20Crimes%20Section%20502.aspx (Feb. 4, 2016).

280 « strategic lawsuit against public participation »

281 West's Ann.Cal.C.C.P § 425.16.available at: http://codes.findlaw.com/ca/code-of-civil-procedure/ccp-sect-425-16.html (Feb. 4, 2016).

IV. VERGLEICHENDE ÜBERSICHT

1. Aufsichtsbehörde

In allen untersuchten Rechtsordnungen besteht eine Aufsichtsbehörde, welche die Respektierung der Datenschutzgesetzgebung durch Private (so in Singapur), in Bezug auf gewisse Daten (so bis Ende 2016 in Japan) oder allgemein (Neuseeland, Argentinien, Südkorea), überwacht. Dies beinhaltet in der Regel das **Vornehmen von Abklärungen auf eigene Initiative** (so insbesondere in Singapur, Südkorea und Argentinien) oder nur **auf Beschwerde** hin (so aktuell in Neuseeland). In Südkorea besteht für Beschwerden ein für allgemeine Belange zuständiges Mediationskomitee sowie eine Behörde, welche u.a. individuelle Datenschutzbeschwerden im IT Bereich durch eine Art Konziliation zu schlichten sucht. Daneben besteht im IT Bereich noch eine separate Aufsichtsbehörde. Neben der Beschwerde an die Aufsichtsbehörde steht in den untersuchten Rechtsordnungen auch der Gerichtsweg offen.

In allen untersuchten Rechtsordnungen stehen Behörden im Rahmen ihrer Aufsichtsbefugnisse auch **Untersuchungsbefugnisse** gegenüber Unternehmen zu, wobei für Zutrittsbefugnisse in der Regel eine vorgängige gerichtliche Genehmigung erforderlich ist.

Neben der Aufsichtsfunktion und der Behandlung von Beschwerden nehmen Datenschutzbehörden in den untersuchten Rechtsordnungen auch **regulatorische und unterstützende Funktionen** (insbesondere im Bereich der Compliance) wahr. In Südkorea handelt es sich dabei um separate Behörden, in den meisten anderen Rechtsordnungen werden diese Funktionen von der Aufsichtsbehörde wahrgenommen.

2. Rechte der Betroffenen

In allen untersuchten Rechtsordnungen haben die Betroffenen grundsätzlich ein **Recht auf Zugang, Korrektur und allenfalls Löschung** der sie betreffenden Daten. Unterschiede bestehen im Bereich der Ausnahmen. So sieht insbesondere die Regelung von Singapur relativ ausführliche Ausnahmen vor, und in Japan reicht zur Ablehnung eines Antrags aus, dass ein Entsprechen unverhältnismässigen Auftrag generieren würde. Auch die Kostenregelungen sind unterschiedlich.

In gewissen Rechtsordnungen bestehen **weitere Ansprüche** der Betroffenen, beispielsweise im Bereich der Informationsrechte. In vergleichender Hinsicht ist auf die Regelung von Japan hinzuweisen, welche gesetzgebungstechnisch die Pflichten der datenbearbeitenden Person in den Vordergrund stellt und kaum von eigentlichen Rechten spricht. Besonders erwähnenswert ist schliesslich ein in Südkorea und Singapur vorgesehenes Recht. So dürfen die betroffenen Personen bei Inanspruchnahme einer Dienstleistung oder Bezug einer Ware darauf bestehen, nicht mehr Daten bekannt zu geben, als dies dafür notwendig ist. Anders formuliert darf das Erbringen einer Dienstleistung oder eines Produkts nicht von der Zustimmung zu einer weitgehenden Datenverarbeitung oder der Mitteilung von persönlichen Daten abhängig gemacht werden.

Die verschiedenen Rechte sind in der Regel auch gerichtlich oder mindestens durch Beschwerde **durchsetzbar**, wobei gerade diesbezüglich verschiedene Reformen oder Reformhaben die Rechte der Betroffenen stärken (sollen). Mediationsverfahren sind insbesondere in Singapur vorgesehen, die Schlichtungsverfahren in Südkorea und Japan entsprechen angesichts der Rolle der Schlichtungsbehörde eher nicht einer eigentlichen Mediation.

Auch die **Schadenersatzbestimmungen** sind nicht einheitlich. Relativ weit geht z.B. Südkorea, indem pauschalierte Schadenersatzbeträge vorgesehen sind.

3. Pflichten der datenbearbeitenden Person

In allen untersuchten Rechtsordnungen müssen datenbearbeitende Personen für die Bearbeitung von Daten die **Zustimmung** der betroffenen Personen einholen und diese auch über den **Zweck der Datenbearbeitung** informieren. Die Datenbearbeitung darf entsprechend nur zu diesem Zweck erfolgen. Lediglich in Japan ist nur für besondere Daten ein ausdrückliches Zustimmungserfordernis vorgesehen. Relativ restriktiv und ausführlich sind die diesbezüglichen Regelungen in Südkorea. Trotz der ähnlichen Grundsätze bestehen also durchaus Unterschiede.

Die datenbearbeitenden Personen haben in verschiedenen Rechtsordnung auch die Pflicht, für die **Sicherheit der Daten** zu sorgen (so in Singapur, Neuseeland, Japan, und Südkorea) und die **Korrektheit der Daten** mindestens in gewissen Fällen zu überprüfen (so in Singapur, Neuseeland, Japan).

Einige Pflichten finden sich nur in wenigen Rechtsordnungen. So sieht z.B. Argentinien die Pflicht zur **Registrierung** von Datensammlungen vor, in Südkorea bestehen eine ähnliche Pflicht für den öffentlichen Sektor. Auch die Pflicht, die betroffenen Personen über ein **Datenleck** zu informieren, findet sich nur in wenigen Rechtsordnungen (so in Südkorea, in Neuseeland wird diese im Rahmen der Reform diskutiert).

Schliesslich sehen verschiedene Rechtsordnungen vor, dass Unternehmen **Richtlinien** zum Datenschutz erlassen müssen.

4. Big Data, Profiling, Internet of Things

In den untersuchten Datenschutzgesetzgebungen finden sich relativ selten Bestimmungen zu Big Data, Data Profiling und dem Internet of Things. So bestehen besondere Regelungen über das **Profiling** soweit ersichtlich nur in Argentinien, wo im Bereich der Werbung das Profiling ohne Zustimmung der betroffenen Personen unter gewissen Voraussegzungen erlaubt zu sein scheint.

Regelungen oder Prinzipien im Zusammenhang mit **Big Data** finden sich in Japan, Singapur und Erwägungen diesbezüglich in Neuseeland. Das auf 2017 in Kraft tretende japanische Gesetz geht hier relativ weit, indem es zwei Kategorien von Datenbearbeitungen vorsieht: persönliche Daten und anonymisierte Daten. Der Begriff der anonymisierten Daten wird dabei im Gesetz definiert, was für Big Data Verarbeiter eine gewisse Rechtssicherheit bringen sollte. Datenbearbeiter haben aber auch bei anonymisierten Daten gewisse Pflichten. In Singapur wird die Problematik der Anonymisierung (als Voraussetzung für eine Big Data Verarbeitung ohne Zustimmung der betroffenen Personen) lediglich in einer unverbindlichen Richtlinie angesprochen, die die verschiedenen Anonymisierungstechniken und das Risiko der Re-identifizierung ausführt. Auch hier soll durch Verweise eine gewisse Rechtssicherheit geschaffen werden. In Neuseeland schliesslich wird lediglich im Zusammenhang mit verschiedenen Prinzipien auf Big Data Verarbeitung hingewiesen, doch haben sich diese im Rahmen der Revisionsarbeiten bislang kaum konkretisiert.

Das **Internet of Things** wird in den verschiedenen untersuchten Regelungen nicht ausdrücklich thematisiert. Eine Bestimmung in Singapur scheint aber auf die Sammlung von Informationen im Internet of Things ausgerichtet. So wird die Zustimmung mit einer Datenerhebung vermutet, wenn Daten freiwillig übermittelt werden und davon ausgegangen werden kann, dass eine Zustimmung hier vernünftigerweise erteilt wird. Im Übrigen finden sich soweit ersichtlich keine konkreten regulatorischen Massnahmen.

5. Massnahmen zur Förderung von Privacy by Design / Privacy By Default

In den meisten untersuchten Rechtsordnungen finden sich kaum Massnahmen zur Förderung von Privacy by Design oder Privacy by Default. Gewisse Behörden beziehen sich aber im Rahmen ihrer Sensibilisierungsfunktionen darauf (so z.B. in Singapur).

Eingehendere Initiativen und regulatorische Ansätze finden sich in **Neuseeland und Argentinien**. So besteht in Neuseeland ein Privacy by Design Panel, welches «best practices» diesbezüglich unterstützen und verbreiten soll, v.a. im öffentlichen Sektor. In Argentinien wird «privacy by design» relativ ausführlich in Richtlinien erwähnt und konkretisiert.

6. Datenportabilität

Soweit ersichtlich besteht in keiner der untersuchten Rechtsordnungen ein Recht auf Datenportabilität oder auch nur Bestimmungen in diesem Zusammenhang. In Argentinien könnte allenfalls ein neues Gesetz zum e-mail Verkehr oder aber durch Auslegung von Grundsätzen der Konsumentenschutzgesetzgebung erlauben, Dienstleistende im Informatikbereich in Ansätzen zur Datenportabilität zu verpflichten.

SCHWEIZERISCHES INSTITUT FÜR RECHTSVERGLEICHUNG

Dr. Lukas Heckendorn Urscheler
Vize-Direktor

Argentinien:	Dr. Alberto Aronovitz
Neuseeland:	John Curran
USA:	Karen T. Druckman
	Wissenschaftliche Mitarbeiter