grundrechte.ch
droitsfondamentaux.ch
dirittifondamentali.ch

Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)

4. April 2017

EJPD

Frau Bundesrätin Simonetta Sommaruga

Vernehmlassung DSG

Per Email zu senden an (als word Datei)

jonas.amstutz@bj.admin.ch

Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Gerne beteiligen wir uns an der Vernehmlassung zur Totalrevision des DSG. grundrechte.ch begrüsst die Stossrichtung der Vorlage. Das Ziel der Revision ist, den Datenschutz zu stärken, die Transparenz zu erhöhen, das Verantwortungsbewusstsein der Datenbearbeiter zu erhöhen und die Aufsicht zu stärken. Die technische Entwicklung und die immer stärkere Vernetzung haben zu einer immensen Erhöhung der Datenmengen geführt und ermöglichen eine überaus komplexe, mächtige Nutzung von Daten. Die mit dem Datenschutz verknüpften Rechte der Betroffenen geraten dadurch immer mehr unter Druck. Eine Stärkung des Datenschutzes tut Not vor dem Hintergrund dieser Entwicklung.

Mit dem revidierten DSG folgt die Schweiz der Entwicklung im europäischen Raum. Die entsprechende EU-Datenschutzgesetzgebung ist aus unserer Sicht als Mindeststandart zu betrachten. Würde dieser unterschritten, wäre die für das Schutzniveau, aber auch aus wirtschaftlicher Sicht erforderliche Gleichwertigkeit mit der EU-Regelung nicht gewährleistet. Punktuell erscheinen aus unserer Sicht zusätzliche Schutznormen als erforderlich, insbesondere, weil die EU-Datenschutzgesetzgebung neuen Qualitäten der Datenbearbeitung, welche sich aus dem Big-Data-Ansatz und der vernetzten Nutzung von Daten ergeben, noch nicht ausreichend gerecht wird.

Nachstehend nehmen wir zu den aus unserer Sicht wichtigsten Bestimmungen im Detail Stellung und legen dar, welcher Änderungen es aus unserer Sicht bedarf, um den Zielen der Revision gerecht zu werden.

Wir bedanken uns für die Gelegenheit, eine Vernehmlassung einzureichen und hoffen, dass unsere Überlegungen und Anträge in den Gesetzgebungsprozess einfliessen können.

RA Viktor Györffy, Präsident von grundrechte.ch

<u>Unsere Stellungnahme im Einzelnen:</u>

Art. 2 - Räumlicher Geltungsbereich

Im Gegensatz zur neuen Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) enthält der vorliegende Entwurf zum revidierten Datenschutzgesetz (DSG) keine besondere Bestimmung zum räumlichen Geltungsbereich. Nach Auffassung des Bundesrates würde bereits das geltende Recht die Möglichkeit bieten, das Gesetz weitgehend auf Situationen mit internationalem Charakter anzuwenden. Er verweist hierzu auf das Bundesgerichtsurteil zu «Google Street View». In diesem Urteil ist, wie vom Bundesrat erwähnt, ein überwiegender Anknüpfungspunkt in der Schweiz gegeben, da Google Inc. mit Hilfe von Google Switzerland GmbH Bilder von Strassenzügen in der Schweiz aufnehmen liess. Diese Situation ist jedoch nicht mit Datenbearbeitern und Inhaber von Datensammlungen - nach heutiger Terminologie - vergleichbar, die komplett aus dem Ausland operieren, sich aber an Personen in der Schweiz richten. Zu erwähnen sind etwa Amazon (unter anderen mit Amazon Web Services), Facebook (auch mit Instagram und WhatsApp), Google (unter anderem mit Gmail, Google Analytics und YouTube), LinkedIn, Microsoft (unter anderem mit Office 365), Twitter, Salesforce und XING.

In all diesen Fällen kann - im Unterschied zur neuen EU-DSGVO - das schweizerische Datenschutzgesetz weiterhin nicht ohne weiteres angewendet werden. Die Auffassung des Bundesrates, das geltende Recht biete bereits die Möglichkeit, das DSG weitgehend auf Situationen mit internationalem Charakter anzuwenden, lässt sich denn auch in der gängigen Praxis nicht nachvollziehen. Ein der neuen EU-DSGVO entsprechendes *Marktortprinzip* muss daher vorgesehen werden. Damit würde dann auch ein in der Schweiz nötiges, vergleichbares Datenschutzrecht gelten.

Art. 3 - Begriffe

Die Streichung des Begriffs und des Konzepts der «Datensammlung» wird ausdrücklich begrüsst. Entscheidend ist die Erschliessbarkeit der Daten: Alle Informationen über eine bestimmte Person, die mit einem vernünftigen Aufwand gefunden werden können, müssen als personenbezogene Daten gelten - unabhängig vom Speicherverfahren oder dem Speicherort.

Ebenfalls scheint begrüssenswert, dass der Begriff «Persönlichkeitsprofil» durch «Profiling» ersetzt wird. **Die Begriffe sind allerdings nicht deckungsgleich**. Wichtig ist, dass der Zweck der Datenbearbeitung durch den Begriff erfasst bleibt, der darauf abzielt, wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen.

Art. 3 lit. a - Personendaten

Der erläuternde Bericht hält in der Definition zum Begriff «bestimmbare Person» folgendes fest:

«Wie auch nach dem aktuellen Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Die zur Verfügung stehenden technischen Möglichkeiten werden in Bezug darauf geprüft, wie hoch der zeitliche und finanzielle Aufwand

für ihre Anwendung ist. Mit Blick auf die immer gezielteren Technologien zur Datenauswertung und deren konstante Weiterentwicklung verschwimmt die Grenze zwischen Personendaten und anderen Daten indes zusehends. Daten, bei denen heute noch eine rein theoretische Möglichkeit der Identifizierung anzunehmen ist, können morgen vielleicht bereits einer bestimmbaren Person zugeordnet werden.»

Es genügt nicht, wenn besonders schützenswerte Personendaten bearbeitet, Dritten bekannt gegeben und veröffentlicht werden dürfen, sofern die Möglichkeit besteht, dass sich diese Personendaten allenfalls zukünftig deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Insbesondere in der Forschung, Planung und Statistik sind Konzepte, wie Differential Privacy seit langem bekannt. Mithilfe von *Noise Injection* lassen sich beispielsweise Daten so verfremden, dass sie zwar statistisch weiterhin auswertbar sind, sie aber keine verlässlichen Rückschlüsse auf Personen mehr zulassen.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist daher in der Botschaft und den Ausführungsbestimmungen festzuhalten.

Art. 3 lit. c Ziff. 4 - Biometrische Daten

Biometrische Merkmale lassen nicht immer eine eindeutige Identifizierung zu. Zudem werden die Möglichkeiten zur automatisierten Erkennung von Personen aufgrund ihrer Stimme, dem Aussehen oder der Art der Fortbewegung noch massiv zunehmen. Wenn folglich biometrische Merkmale zur Identifizierung geeignet sind oder zur Identifikation bearbeitet werden, müssen sie als besonders schützenswerte Personendaten gelten.

Das Wort «eindeutig» ist daher zu streichen.

Art. 4 Abs. 2 - Verhältnismässigkeit

«Datenvermeidung» und «Datensparsamkeit» fehlen als explizite Grundkonzepte und als Teil der notwendigen Verhältnismässigkeit (s. Art. 4 Abs. 6). **Der Absatz ist zu ergänzen mit: *«Die Bearbeitung personenbezogener Daten sowie die Auswahl und Gestaltung der Datenbearbeitungssysteme sind dahin gehend auszurichten, dass so wenig personenbezogene Daten wie möglich von der Bearbeitung betroffen sind.»***

Art. 4 Abs. 3 - Zweckbestimmung

Da die Weiterverarbeitung von Personendaten zu kompatiblen Zwecken erlaubt sein soll, muss der Zweck - wie im Vorentwurf vorgesehen - für die betroffene Person klar erkennbar sein.

Übermittelt die betroffene Person (wie beispielhaft im erläuternden Bericht festgehalten) ihre Adresse im Hinblick auf den Erhalt einer Kundenkarte, so mag die Weiterbenutzung dieser Adresse durch das betreffende Unternehmen zu Werbezwecken im Rahmen einer anfänglich erkennbaren Zweckbestimmung liegen. Findet die Übermittlung im Rahmen einer Bestellung (online oder nicht) statt, sollte jedoch nicht davon ausgegangen werden können.

An der Bestimmung soll - wie im Vorentwurf vorgesehen - festgehalten werden.

Art. 4 Abs. 6 - Einwilligung

Die Bestimmung ist nur zusammen mit den Grundsätzen der Datenvermeidung und der Datensparsamkeit wirksam. Dies zeigen aktuelle Beispiele:

Ein «Cookies-Balken», der nicht abgelehnt werden kann, ist für die betroffene Person wenig hilfreich. Es muss auch jederzeit die Möglichkeit des Widerrufs einer Einwilligung gegeben sein. Zudem müssen Personen in einem Abhängigkeitsverhältnis vor unwillentlich abgegebenen und unverhältnismässigen Zustimmungen geschützt werden (zum Beispiel Arbeitnehmer vor Pauschalvollmachten bei der Aufnahme in eine Kranken- oder Unfallversicherung oder Pensionskasse).

An den Grundsätzen der Datenvermeidung und der Datensparsamkeit muss entsprechend festgehalten werden. Es darf auch nicht bereits davon ausgegangen werden, dass eine ausdrückliche Einwilligung vorliegt, wenn ein entsprechendes Kästchen - womöglich mit einer missverständlichen Beschriftung - bereits vorausgefüllt ist und auf die Schaltfläche «weiter» geklickt wird. **Eine Verdeutlichung in Art. 4. Abs. 2 ist daher vorzunehmen.**

Art. 8 - Empfehlungen der guten Praxis

Das Prinzip der «Empfehlungen der guten Praxis» wird begrüsst. Dieser Vorschlag ist insbesondere einer (alleinigen) Selbstregulierung durch die Branchen vorzuziehen, da erst der Einbezug interessierter und betroffener Kreise, d. h. sowohl der Anwender wie auch der Anbieter von Produkten und Dienstleis-tungen, zu angemessenen Regelungen der Empfehlungen der guten Praxis führen.

Art. 11 - Sicherheit von Personendaten

Der Artikel im Vorentwurf ist wie der bestehende Art. 7 DSG vage. Er hält insbesondere keine Schutzziele fest. **Wir erwarten vom Bundesrat, dass die erwähnten technischen und organisatorischen Schutzmassnahmen mindestens auf Verordnungsstufe konkretisiert werden.**

Art. 12 - Daten einer verstorbenen Person

Die neue Bestimmung über «Daten einer verstorbenen Person» wird begrüsst.

Art. 13 Abs. 3 und 4 - Informationspflicht bei der Beschaffung von Personendaten

Die Bestimmungen gilt auch für die Auskunftspflicht nach Art. 20 Abs. 2 lit. g. Zur Erfüllung der *Informationspflicht* ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger ausreichend. Die *Auskunftspflicht* hingegen muss aber neben den Daten auch die Empfänger der Daten - und nicht nur deren Kategorien umfassen. **Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist daher (in Art. 20) sinnvoll.**

Art. 14 Abs. 3 und 4 - Ausnahmen von der Informationspflicht und Einschränkungen

Die Einschränkungen und Bestimmungen gelten speziell für die Auskunftspflicht nach Art. 21. Sind von der *Auskunftspflicht* jedoch «überwiegende Interessen Dritter» betroffen, sollten diese Angaben geschwärzt werden, damit keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf

zu verzichten).

Daher ist Abs. 3 wie folgt abzuändern:

Abs. 3: *«Der Verantwortliche kann die Übermittlung der Informationen einschränken,*

aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisiert die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.»

Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie beispielsweise dem Nachrichtendienstgesetz, zu regeln.

Abs. 4 lit. b: *«[…] wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.»*

Die Abs. 3 und 4 wären unseres Erachtens in Art. 21 besser aufgehoben.

Art. 15 Abs. 1 - Informationspflicht bei einer automatisierten Einzelentscheidung

Es ist zu befürchten, dass in der Praxis von einer Information über eine automatisierte Einzelentscheidung abgesehen werden dürfte, wenn eine rein theoretische Möglichkeit zur Einflussnahme besteht. Falls nicht, könnte sie gar zur Umgehung geschaffen werden.

In den nicht offensichtlichen Fehlbeurteilungen ist zudem nur die betroffene Person in der Lage, die Richtigkeit der automatisierten Einzelentscheidung abzuschätzen. Die Auswirkungen können aber dennoch erheblich sein.

Das Wort «ausschliesslich» ist daher zu streichen.

Alternativen: Es könnte auch der Beauftragte zur Prüfung herangezogen werden, ob es sich beim angewandten Entscheidungsprozess um eine automatisierte Einzelentscheidung im Sinne von Art. 15 handelt. Und/oder das angewandte Verfahren müsste im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 16 regelmässig auf seine Wirksamkeit geprüft werden.

Art. 15 Abs. 2 - Anhörungspflicht bei einer automatisierten Einzelentscheidung

Die betroffene Person muss sich nicht nur zur automatisierten Einzelentscheidung und den bearbeiteten Daten äussern können. Sie muss sich gegebenenfalls auch ein Bild des angewandten Verfahrens machen können. **Da dies sinngemäss auch für das Profiling im Sinne von Art. 3 lit. f gelten muss, ist eine Regelung in der Auskunftspflicht nach Art. 20 vorzusehen.**

Art. 16 - Datenschutz-Folgenabschätzung

Die Regelung der Datenschutz-Folgeabschätzung wird begrüsst. Dies entspricht dem gewählten, ausdrücklich risikobasierten Ansatz im revidierten DSG.

Art. 16 Abs. 5 (neu) - Periodische und rückwirkende Datenschutz-Folgenabschätzung

Eine einmalige Datenschutz-Folgeabschätzung ist in einem schnell ändernden Umfeld ungenügend. Es gilt explizit festzuhalten, dass diese periodisch oder bei Änderung der Risiken erneut vorzunehmen sei.

Zudem müssen Datenschutz-Folgenabschätzungen auch rückwirkend, wie in Art. 59 lit. a vorgesehen, für bereits bestehende Datenbearbeitungen durchgeführt werden:

«Die Datenschutz-Folgeabschätzung muss vom Verantwortlichen oder vom Auftragsbearbeiter bei einer Änderung des Risikos oder spätestens alle fünf Jahre wiederholt werden. Eine Benachrichtigung des Beauftragten durch den Verantwortlichen und eine Beurteilung durch den Beauftragten erfolgt bei einem abweichenden Ergebnis der Datenschutz-Folgenabschätzung oder einer Anpassung der Massnahmen.»

Art. 16 Abs. 1, 3, 4 sowie 5 (neu) - Datenschutz-Folgeabschätzung für Gesetzeserlasse

Art. 59 lit. a - Übergangsbestimmung

Nicht nur private Verantwortliche oder Bundesorgane sollen zu Datenschutz-Folgeabschätzungen verpflichtet werden. Bereits beim Erlass neuer Gesetze muss dem Datenschutz und dem Schutz der Persönlichkeitsrechte mehr Beachtung geschenkt werden. Entsprechend ist auch in diesen Fällen eine Datenschutz-Folgeabschätzung zu erstellen und bei Änderungen zu wiederholen.

Auch diese Datenschutz-Folgenabschätzungen müssen rückwirkend für bereits bestehende Gesetze (spätestens fünf Jahre nach Inkrafttreten des DSG) durchgeführt werden:

«[…] der Verantwortliche oder der Auftragsbearbeiter»* ist jeweils zu ergänzen: *«der Verantwortliche, der Auftragsbearbeiter oder Gesetzgeber».

Art. 16 Abs. 6 (neu): Evaluation von Gesetzeserlassen

Gesetze, welche eine Überwachung von Personen beinhalten, werden mit einem «Verfallsdatum» versehen. Sie müssen nach den ersten fünf Jahren seit Inkrafttreten zwingend einer Evaluation, welche die Wirksamkeit und Verhältnismässigkeit prüft, unterzogen werden. Das Resultat bestimmt darüber, ob das Gesetz weiter angewendet werden kann. **Wir schlagen daher folgende Ergänzung vor:**

«Handelt es sich um ein Gesetz, welches eine Überwachung von Personen beinhaltet, ist es auf eine Anwendungsdauer von fünf Jahren zu beschränken. Eine Evaluation der Wirksamkeit und Verhältnismässigkeit bestimmt darüber, ob das Gesetz weiter angewendet werden darf.»

Alternativ kann das Resultat der Evaluation auch als Grundlage für eine zwingende Neuberatung durch das Parlament verwendet werden.

Art. 17 Abs. 4 - Meldung von Verletzungen des Datenschutzes

Der Auftragsbearbeiter muss den Verantwortlichen nicht nur über eine unbefugte Datenbearbeitung, sondern auch - wie in Abs. 1 für den Verantwortlichen festgehalten - über einen Verlust von Daten informieren. **Der Absatz muss daher lauten: *«Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte***

Datenbearbeitung oder den Verlust von Daten.»

Art. 17 Abs. 5 (neu) - Meldung von Verletzungen des Datenschutzes durch Internetkriminalität

Beim Verlust von Daten durch Internetkriminalität sollte neben dem Beauftragten und den betroffenen Personen auch die Melde- und Analysestelle Informationssicherung MELANI informiert werden. Durch das Wissen aus konkreten Fällen ist es ihr möglich, Gefahren für Schweizer Unternehmen zu erkennen, ein Gefahrenbild zu erstellen und Massnahmen zu empfehlen. Entsprechend ist der Beauftragte zu ermächtigen, MELANI zu informieren: ***«Bei Verlust von Daten informiert der Beauftragte die für die Sicherheit von Computersystemen und des Internets zuständige Melde- und Analysestelle Informationssicherung MELANI.»***

Art. 18 - Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sind wichtige Prinzipien und sorgen erst dafür, dass die Einwilligung der betroffenen Person nach Art. 4 Abs. 6 auch tatsächlich eingeholt wird. **Ein Verstoss muss sanktioniert sein/bleiben.** Zudem müssen Massnahmen für Daten-schutz durch Technik und datenschutzfreundliche Voreinstellungen **auch rückwirkend, wie in Art. 59 lit. b vorgesehen, für bereits bestehende Datenbearbeitungen umgesetzt werden.**

Art. 19 lit. a - Weitere Pflichten

Gemäss dem erläuternden Bericht wird dadurch für Private die bisherige Verpflichtung ersetzt, Datensammlungen beim Beauftragten zu registrieren. Dies entspricht nicht den Anforderungen aus dem Übereinkommen SEV 108 und der EU-DSGVO. **Vielmehr muss auch nachgewiesen werden können, dass die Datenschutzbestimmungen eingehalten werden. Dies geht über ein Register der Datenbearbeitungen hinaus. Dies ist zu verdeutlichen.**

Art. 20 - Auskunftsrecht

Das Auskunftsrecht ist ein zentrales Element des Datenschutzes und schafft die Grundlage für die Durchsetzung weiterer Rechtsansprüche der betroffenen Personen.

Art. 20 Abs. 1 - Auskunftsrecht und Kosten

Die Auskunft ist - wie im Vorentwurf vorgesehen - kostenlos vom Verantwortlichen zu leisten.

Art. 20 Abs. 2 lit. c - Auskunftsrecht zur Rechtsgrundlage

Gegenüber der Bestimmung im geltenden DSG wurde hinsichtlich dem Auskunftsrecht die Angaben zur Rechtsgrundlage gestrichen. In den Erläuterungen lässt sich keine Begründung hierzu finden. Eine Angabe zur Rechtsgrundlage dient dazu, dass die betroffene Person ihre Rechte nach dem DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.

Wir schlagen daher vor, lit. c. zu ergänzen: «…der Zweck der Bearbeitung und die Rechtsgrundlage;»

Art. 20 Abs. 2 lit. g - Auskunftsrecht und Informationspflicht

Zur Erfüllung der *Informationspflicht* ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger gemäss Art. 13 Abs. 3 und 4 ausreichend. Die *Auskunftspflicht* hingegen muss aber neben den Daten auch die Empfänger der Daten - und nicht nur deren Kategorien umfassen. Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist daher sinnvoll. **Lit. g und h (neu) sind wie folgt zu formulieren:** ***«g. gegebenenfalls Empfängerinnen und Empfänger der Personendaten;***

h. gegebenenfalls die Identität und Kontaktdaten des Auftragsbearbeiters der Personendaten.»

Art. 20 Abs. 3 - Auskunftsrecht und Entscheidungen

Bereits heute finden massenhaft automatisierte Einzelentscheidungen - die ausschliesslich auf Algorithmen beruhen und ohne menschliches Eingreifen getroffen werden - auf Grund von Personendaten statt. Beispiele sind Social Media-Plattformen, personalisierte Werbung und Beeinflussung durch Microtargeting.

In Zukunft werde noch viel mehr persönliche Daten aus dem «Internet of Things», vom Strom-Smart-Meter über Mobilitäts- und Gesundheitsdaten bis zu Sensordaten aus «intelligenten» Fernsehern zur automatisierten Auswertung zur Verfügung stehen.

Für die Nachvollziehbarkeit sind Informationen über die verwendeten Algorithmen wichtig. Die Bestimmung greift daher zu kurz und muss grundsätzlich ein Auskunftsrecht über die Bearbeitung mit Algorithmen enthalten. Die Mechanismus Transparenz muss in geeigneter Form (beschreibend oder als Algorithmus selber) erfolgen.

Neue Formulierung für Art. 20 Abs. 3:

«Werden Personendaten automatisiert bearbeitet, erhält die betroffene Person das Ergebnis und Informationen über das Zustandekommen des Ergebnisses, bei einer automatisierten Einzelent-scheidung zusätzlich die Auswirkungen der Entscheidung, mitgeteilt.»

Neue Formulierung für Art. 20 Abs. 2 lit. e: ***«[…] das Vorliegen einer automatisierten Bearbeitung;»***

Art. 20 Abs. 7, 8, 9 und 10 (neu) - Datenauskunft und Daten Portabilität

Bis anhin ist es für Betroffene nur umständlich und mit viel zeitlichem Aufwand möglich, das Datenauskunftsrecht wahrzunehmen. Die Anfragen werden von den Verantwortlichen oft (lange) ignoriert, unvollständig gewährt und beinhalten lediglich einige ausgedruckte Screenshots. Auch die neuen Bestimmungen zum Auskunftsrecht enthalten keine zeitlichen und formellen Vorgaben, keine Pflicht zur Vollständigkeitsbestätigung und keine Angaben zu den Rechten der Betroffenen, einschliesslich Angaben entsprechend einer Rechtsmittelbelehrung. Diese wären zum Ausgleich des Machtgefälles wichtig.

Das Recht auf Datenportabilität ist im vorliegenden Entwurf nicht vorgesehen. Dies ist unverständlich, da Schweizer Firmen, falls sie sich an Personen in der EU richten, dies nach EU-Recht einführen müssen. Ein Verzicht nützt den Unternehmen nichts, schwächt aber die Konsumentenrechte in der Schweiz. **Wir schlagen Folgende Ergänzungen vor:**

Abs. 7 (neu): ***«Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt. Ist die Informationsbeschaffung mit unverhältnismässigem Aufwand verbunden, erhält die betroffene Person nach spätestens 30 Tagen eine Übersicht zu den Kategorien und dem Zweck der bearbeiteten Daten. Die betroffene Person bestimmt, zu welchen Kategorien die vollständige Auskunft zu erteilen ist.»***

Abs. 8 (neu): ***«Die Auskunft hat in der Regel elektronisch und in einem Format zu erfolgen, das sich zur Weiterverarbeitung eignet, es sei denn die Bearbeitung der Daten findet nicht elektronisch statt.»***

Abs. 9 (neu): ***«Die Vollständigkeit und Korrektheit der Datenauskunft ist zu bestätigen.»***

Abs. 10 (neu): ***«Die Datenauskunft enthält Angaben zu den Betroffenenrechten.»***

Art. 21 - Einschränkung des Auskunftsrechts

Die Ausnahmen zur *Informationspflicht* und Einschränkungen aus Art. 14 sollten von der Auskunftspflicht getrennt werden. Sind von der *Auskunftspflicht* «überwiegende Interessen Dritter» betroffen (bei denen die betroffene Person durch die Information über die Datenbearbeitung auch Informationen über Drittpersonen erhält und dadurch die Interessen dieser Drittpersonen beeinträchtigt werden können), müssen diese Angaben so «geschwärzt» werden, dass keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. **Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten).**

Übernahme von Art. 14 Abs. 3:

Abs. 1: ***«Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisieren die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.»***

Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie zum Beispiel dem Nachrichtendienstgesetz, zu regeln.

Übernahme von Art. 14 Abs. 4:

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

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

b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.»

Der zweite Satz in Art. 21 Abs. 2 ist damit überflüssig. Der Absatz lautet neu verkürzt:

«Der Verantwortliche muss begründen, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt.»

Art. 22 und Art. 24 Abs. 2 lit. d - Medien

Die Medienlandschaft hat sich in den letzten Jahren dramatisch gewandelt. Traditionelle Zeitungen verschwinden, Online-Angebote nehmen deren Platz ein und Betreiber von Blogs tragen immer mehr zur journalistischen Arbeit bei. Die Einschränkung des Auskunftsrechts für Medienschaffende sollte sich daher stärker am Zweck der Datenbearbeitung als an einem «periodischen Medium» oder dem Beruf des «Medienschaffenden» orientieren.

Auf die Anforderungen bezüglich «beruflich» und «periodisch» ist deshalb zu verzichten.

Art. 24 Abs. 2 lit. e - Anonymisierung usw.

Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmbar*. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).

Art. 25 - Rechtsansprüche

Verletzungen der Auskunfts-, Melde- und Mitwirkungspflichten, der Sorgfaltspflichten sowie der beruflichen Schweigepflicht sollen gemäss vorliegendem Entwurf nach Art. 50 bis 52 bestraft werden können. Nicht strafrechtlich relevant blieben Persönlichkeitsverletzungen durch Datenbearbeitungen und Verstösse gegen die Datenbearbeitungsgrundsätze. **Verstösse gegen diesen Kernbereich des Datenschutzes müssten aber ebenfalls sanktioniert werden können. Dies ist entsprechend in Kapitel 8 «Strafbestimmungen» vorzusehen (siehe Art. 50).**

Bei Verstössen gegen das Datenschutzrecht ist in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen ist weniger relevant. **Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).**

Art. 25 Abs. 1 lit. c - Recht auf Vergessenwerden

Im Entscheid zum «Recht auf Vergessenwerden», wie ihn der Europäische Gerichtshof gegenüber Google gefällt hat, geht es nicht primär um das Löschen oder Vernichten von Daten. Vielmehr musste der Suchalgorithmus von Google dahingehend angepasst werden, dass Suchergebnisse zu einem bestimmten Ereignis bei der Suche nach einer Person nicht mehr angezeigt werden. **Der Begriff des «Löschens» sollte entsprechend mit diesem Bezug erläutert werden.**

Art. 25 Abs. 4 (neu) - Verbands- und Sammelklagen

Bereits heute kann sich der Beauftragte aufgrund knapper Ressourcen nur auf wenige exemplarische Fälle von (möglichen) Datenschutzverletzungen konzentrieren. Mit dem totalrevidierten Datenschutzgesetz sollen dem Beauftragten neue Aufgaben zufallen. Gleichzeitig dürften die Ressourcen nicht nennenswert aufgestockt werden.

Auch mit dem neuen Gesetz bleibt die Grundschwierigkeit bestehen, die zustehenden Rechte in der Praxis durchsetzen zu können. In Art. 25 ist zum Beispiel nicht vorgesehen, dass Verstösse gegen den Kernbereich des Datenschutzes der Schwere entsprechend sanktioniert werden können.

Als einzelner Kunde oder als Arbeitnehmer in einem Abhängigkeitsverhältnis ist es schwierig gegen (mögliche) Datenschutzverstösse vorzugehen. Ein wirkungsvolles Mittel wäre eine Regelung zur kollektiven Rechtsdurchsetzung (Erweiterung des Verbandsklagerechts und Einführung einer Sammelklage bzw. eines Sammelvergleichs).

Gemäss dem erläuternden Bericht sollen die Instrumente der kollektiven Rechtsdurchsetzung im Rahmen der Umsetzung der Motion 13.3931 Birrer-Heimo in einem grösseren, möglichst Sektor übergreifenden Kontext geprüft werden. In der Stellungnahme des Bundesrates zur Motion ist zu entnehmen:

«Neben der Verbesserung im Rahmen der bereits bestehenden Instrumente erachtete er dabei die Einführung neuer, eigenständiger Instrumente der kollektiven Rechtsdurchsetzung für denkbar, namentlich die Schaffung eines Muster- oder Testverfahrens sowie eines Gruppenklage- oder Gruppenvergleichsverfahrens. Vor diesem Hintergrund ist der Bundesrat bereit, entsprechende punktuelle Gesetzesänderungen vorzuschlagen oder im Rahmen laufender Gesetzgebungsarbeiten zu berücksichtigen. In diesem Zusammenhang sei beispielsweise auf die laufende Aktienrechtsrevision sowie die Arbeiten an einem Finanzdienstleistungsgesetz (Fidleg) hingewiesen. Dagegen erachtet es der Bundesrat nicht als opportun, einen eigenständigen Erlass zum kollektiven Rechtsschutz (‹Sammelklagengesetz›) zu erarbeiten.»

Folgerichtig muss im neuen DSG eine Regelung zur kollektiven Rechtsdurchsetzung (Verbands-klagerecht und Sammelklage), analog beispielsweise zum UWG, vorgesehen sein:

Art. 25 Abs. 4 (neu): ***«Klageberechtigt sind auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss unter anderem dem Datenschutz widmen.»***

Art. 25 Abs. 5 (neu) - Beweislastumkehr

Eine unrechtmässige Bearbeitung von Daten ist nur schwierig und/oder in einem langwierigen Verfahren nachzuweisen, wenn die Klärung des Sachverhalts auf die Mitarbeit und Informationen der beschuldigten Partei angewiesen ist. In schwerwiegenden Fällen muss die Beweislast daher umgedreht werden.

Beispiel: Ein Online-Dienstleister bearbeitet Daten «im Auftrag» der Personen, die den Dienst nutzen. Dies können zum Beispiel deren Fotos, das Adressbuch und die Kontakte innerhalb der Plattform sein. Als Dienstanbieter verwendet er diese Daten aber ebenfalls für sich selbst oder für Dritte, zum Beispiel für Werbung. Und wiederum verwendet er diese Daten «im Auftrag» für andere Personen, die den Dienst nutzen, um Kontakte zu verknüpfen oder Personen in deren Fotos zu erkennen. Betroffen von dieser vielfältigen Datenbearbeitung sind aber nicht nur die

beauftragenden Personen, sondern auch unbeteiligte Dritte, zum Beispiel auf den Fotos oder in den Adressbüchern.

Der Anbieter ist zu einer angemessenen Mithilfe zu verpflichten. Den Beweis einer rechtmässigen Bearbeitung kann durch den Verantwortlichen beispielsweise durch Darlegung der Einhaltung von Empfehlungen der guten Praxis erbracht werden. Andernfalls muss davon ausgegangen werden, dass eine unrechtmässige Bearbeitung vorliegt. **Daher schlagen wir folgende Präzisierung vor:**

«Besteht der Verdacht auf eine schwerwiegende und systematische Verletzung der Persönlichkeit, ist der Verantwortliche verpflichtet, die rechtmässige Bearbeitung der Daten nachzuweisen.»

Art. 27 Art. 2 - Rechtsgrundlagen

Das Profiling birgt immer besondere Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen. Daher muss für ein Profiling immer eine Grundlage in einem formellen Gesetz gegeben sein; **eine Regelung in einem Gesetz im materiellen Sinn ist nicht ausreichend.**

Art. 29 Abs. 4 - Bekanntgabe von Personendaten

Wir lehnen die Ausnahme gemäss Art. 29 Abs. 4 ab. Die Annahme, solche Grundangaben zur Identifizierung einer Person könnten ohnehin auf einfachem Weg in Erfahrung gebracht werden, ist nicht zulässig. Gerade in einem digitalen Kontext stellt beispielsweise das Geburtsdatum ein wichtiges Identitäts- und Sicherheitsmerkmal dar.

Art. 29 Abs. 5 - Bekanntgabe von Personendaten

Die Adressangaben beispielsweise aus der Switch-WHOIS-Datenbank werden regelmässig automatisiert ausgelesen und unrechtmässig weiterbearbeitet. Bei der Zugänglichmachung von Personendaten mittels automatisierter Informations- und Kommunikationsdienste muss entsprechender Missbrauch wirkungsvoll verhindert werden.

Abs. 5 sollte daher ergänzt werden: *«Ein missbräuchliches, insbesondere automatisiertes Beschaffen der Daten durch Dritte ist wirkungsvoll zu verhindern.»*

Art. 30 Abs. 2 - Widerspruch gegen die Bekanntgabe von Personendaten

Die historische Rechtsabwägung nach lit. b ist nicht mehr nötig und zu streichen.

Abs. 2: ergänzen: *«Das Bundesorgan weist das Begehren ab, wenn eine Rechtspflicht zur Bekanntgabe besteht.»*

Art. 32 Abs. 1 - Datenbearbeitung für Forschung, Planung und Statistik

Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmbar*. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren.

Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders

schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).

Art. 34 Abs. 3bis (neu) - Verbands- und Sammelverfahren

Analog zu Art. 25 Abs. 4 (neu) sind auch die Voraussetzungen für Verbands- und Sammelverfahren zu schaffen: ***«Ansprüche und Verfahren stehen ebenso Organisationen von gesamtschweizerischer oder regionaler Bedeutung zu, die sich statutengemäss unter anderem dem Datenschutz widmen.»***

Art. 37 Abs. 1 - Ernennung und Stellung

Der Beauftragte kontrolliert unter anderem auch die Verwaltung. Er sollte daher unabhängig vom Bundesrat und der übrigen Exekutive beziehungsweise Verwaltung gewählt werden:

«Die oder der Beauftragte wird von der Bundesversammlung für eine Amtsdauer von vier Jahren gewählt.»

Art. 41 - Untersuchung

Die erweiterten Untersuchungsbefugnisse werden begrüsst. Diese entsprechen auch den Vorgaben von Europarat und EU. Allerdings geben diese eine Behandlungspflicht (und nicht nur eine Möglichkeit) durch den Beauftragten vor. Der anzeigenden Person sollte ein Recht auf einen Entscheid und eine Anfechtmöglichkeit zugestanden werden:

Abs. 1: «*Der Beauftragte eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung*

gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.»

Abs. 5: Ist verbindlicher zu formulieren und eine Behandlungsfrist festzuhalten.

Art. 50 bis 52 - Strafbestimmungen

Verletzungen der Auskunfts-, Melde- und Mitwirkungspflichten, der Sorgfaltspflichten sowie der beruflichen Schweigepflicht sollen gemäss vorliegendem Entwurf nach Art. 50 bis 52 bestraft werden können. Nicht strafrechtlich relevant blieben Persönlichkeitsverletzungen durch Datenbearbeitungen und Verstösse gegen die Datenbearbeitungsgrundsätze gemäss Art. 25. **Verstösse gegen diesen Kernbereich des Datenschutzes müssten aber ebenfalls sanktioniert werden können. Dies ist entsprechend in Kapitel 8 «Strafbestimmungen» vorzusehen.**

Bei Verstössen gegen das Datenschutzrecht ist in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen ist weniger relevant. Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).

Art. 50 und 51 - Verwaltungssanktionen

Die aktuell bereits bestehenden Strafbestimmungen im DSG haben sich nicht bewährt: Entsprechende Urteile sind fast gänzlich unbekannt.

Der Entwurf sieht vor, auf die in der EU-DSGVO verankerten Verwaltungssanktionen zu verzichten. Stattdessen sollen die Strafbarkeitsbestimmungen ausgebaut und insbesondere der Strafrahmen stark ausgedehnt werden. Die Wirksamkeit strafrechtlicher Sanktionen vermag jedoch offenkundig nicht an jene von Verwaltungssanktionen heranzureichen. Strafrechtliche Sanktionen können nur greifen, soweit der Rechtsverstoss einer Person individuell zugeordnet werden kann. Die Höhe der Busse orientiert sich wesentlich am individuellen Verschulden dieser Person und ist auch durch ihre persönlichen finanziellen Verhältnisse limitiert.

Im Rahmen von Verwaltungssanktionen kann ein Verstoss viel umfassender gewürdigt und sanktioniert werden. Anders als bei einer strafrechtlichen Verfolgung fällt dabei jede in einer Organisation feststellbare Pflichtverletzung ins Gewicht. Ihre Auswirkungen können umfassend berücksichtigt werden, ebenso die wirtschaftliche Potenz der betroffenen Organisation und die von ihr - allenfalls unter Inkaufnahme von datenschutzrechtlichen Pflichten - erzielten Gewinne.

Nach Art. 30 Abs. 1 StGB kann auch nur die Person, die durch eine Tat verletzt worden ist, die Bestrafung des Täters beantragen. Bei der Pflicht zur Dokumentation von Datenbearbeitungen oder der Durchführung einer Datenschutz-Folgenabschätzung dürfte jedoch oft unklar sein, wer durch eine Unterlassung konkret betroffen ist.

Insbesondere bei gravierenden Verstössen gegen das Datenschutzrecht ist zudem in der Regel von einem Organisationsverschulden auszugehen, bei dem unterschiedliche Akteure in vielfältigen Funktionen und verteilt über verschiedene Gremien und Hierarchien beteiligt sind. Untersuchungen, die darauf ausgerichtet sind, den Grad des schuldhaften Verhaltens von einzelnen Akteuren festzustellen, scheinen wenig sinnvoll. Dabei droht die Sicht auf das Ganze verloren zu gehen.

Insbesondere bei Verstössen von grosser Tragweite wird der Beauftrage mit grosser Wahrscheinlichkeit zugezogen. Das Argument des Bundesrats ist daher falsch, dass die Organisation des Beauftragten verändert werden müsste, um Verwaltungssanktionen durch den Beauftragten aussprechen zu können, worauf insbesondere mit Blick auf die Kosten verzichtet wurde. Es ist auch ökonomisch sinnvoll, die Kompetenz für solche komplexen Untersuchungen zentral zu halten. Im Strafrecht droht zudem die Gefahr von Bauernopfern.

Die EU sowie der Europarat verlangen ausdrücklich auch Verwaltungssanktionen, die der Beauftragte verhängen kann. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Strafrechtliche Massnahmen vermögen a priori nicht die Wirksamkeit und Abschreckung zu gewährleisten, welche denjenigen von Verwaltungsmassnahmen entsprechen.

Um nicht zuletzt die Angemessenheit hinsichtlich der EU-DSGVO zu gewährleisten, erscheint es daher (allenfalls zusätzlich zu den vorgeschlagenen Strafbestimmungen) als erforderlich, Verwaltungssanktionen durch den Beauftragten vorzusehen. Die Konzepte sind nicht neu. Die Schweiz kennt sie zum Beispiel aus der Wettbewerbskommission und der ComCom.

Art. 50 und 51 - Strafmass

Auch gegenüber grossen Unternehmen, die unter Umständen mehrere Milliarden Dollar Gewinn pro Quartal erzielen, müssen Sanktionen genügend abschreckend sein. Die in der EU drohenden Strafen von 20 Mio. Euro oder 4 % des Umsatzes (was entsprechend höher ist) scheinen angemessen. Mit den im Entwurf vorgesehenen Bussen ist eine vergleichbare Wirksamkeit und Abschreckung gegenüber grossen Unternehmen nicht zu erzielen.

Art. 52 - Verletzung der beruflichen Schweigepflicht

Mit der Bestimmung würde (im Bereich der Personendaten) ein Tatbestand für Mitarbeiter von Privatfirmen geschaffen, welcher der Amtsgeheimnisverletzung bei staatlichen Angestellten entspricht. **Dies könnte negative Auswirkungen für Informanten (Whistleblower) haben, welche berechtigterweise auf Missstände in ihren Unternehmen aufmerksam machen wollen. Wir lehnen die neue Bestimmung deshalb ab.**

Art. 57 Abs. 1 - Vollzug durch die Kantone

Die Unterstellung der Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unter das Bundesgesetz über den Datenschutz wird begrüsst.

Zivilprozessordnung (ZPO)

Die Erleichterungen für die private Rechtsdurchsetzung durch den Verzicht auf Gerichtskosten und Leistung einer Sicherheit werden begrüsst.

Ermächtigungen zur Datenbearbeitung in anderen Gesetzen

Das totalrevidierte Datenschutzgesetz beruht über weite Strecken auf denselben Grundprinzipien wie das bisherige Recht. Die Tragweite neu geschaffener Vorschriften ist grösstenteils aus sich selbst genügend klar. Unmittelbarer Änderungsbedarf in Einzelgesetzen besteht somit nur beschränkt. Jedenfalls ist die Totalrevision des Datenschutzgesetzes nicht der richtige Ort, um spezifische Bestimmungen zur Bearbeitung von Personendaten in einzelnen Bundesgesetzen zu schaffen oder abzuändern. Sofern der Bundesrat hier Änderungen anstrebt, sind diese im Rahmen einer Revision des jeweiligen Bundesgesetzes zu diskutieren und allenfalls zu beschliessen. Nur so erscheint als gewährleistet, dass die im Rahmen der konkreten Materie vorzunehmenden Abwägungen im Gesetzgebungsprozess mit der erforderlichen Sorgfalt getroffen werden.

Abgesehen von redaktionellen Änderungen, welche sich aus der neuen Terminologie ergeben, ist daher im Rahmen dieser Revision von der Änderung spezifischer datenschutzrechtlicher Bestimmungen in Einzelgesetzen abzusehen. Namentlich sind sämtliche Bestimmungen, mit denen Ermächtigungen zur Datenbearbeitung in anderen Gesetzen geschaffen oder ausgedehnt werden, zu streichen. Dies betrifft insbesondere die Ermächtigungen zum Profiling. In den Bundesgesetzen müssen individuelle, klare und strenge Rahmenbedingungen für das Profiling vorgesehen werden.