privatim
die schweizerischen datenschutzbeauftragten
les préposé(e)s suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Basel, 9. März 2017

Chance zur Stärkung des Datenschutzes

Zusammenfassung der Stellungnahme von privatim zum Vernehmlassungsentwurf für ein totalrevidiertes Datenschutzgesetz des Bundes

privatim begrüsst den Vorentwurf zur Totalrevision des Datenschutzgesetzes (DSG). Er ist eine *Chance, das Datenschutzrecht den aktuellen Herausforderungen anzupassen*, um den zunehmenden Risiken für die Grundrechte und Persönlichkeitsrechte der betroffenen Personen zu begegnen. privatim legt Wert auf klare Rechtsgrundlagen. Für die datenbearbeitenden Stellen müssen die Rahmenbedingungen und ihre Pflichten eindeutig sein; die betroffenen Personen müssen wissen, welche Rechte sie haben und wie sie diese tatsächlich durchsetzen können. Unter diesem Blickwinkel sind die Bestimmungen in Bezug auf deren Wirkung für die datenbearbeitenden Stellen und die betroffenen Personen fassbar zu machen. Hieraus ergeben sich für privatim die folgenden allgemeinen und spezifischen Bemerkungen zum Vorentwurf zur Totalrevision des DSG:

Allgemeine Bemerkungen

Aufteilung in zwei Gesetze

Das VE-DSG – wie auch das geltende DSG – stellen allgemeine Datenschutzbestimmungen auf, die sowohl für den privaten Datenbearbeiter («private Personen») wie auch für öffentliche Organe («Bundesorgane») gelten. Wir schlagen vor, den privatrechtlichen und den öffentlich-rechtlichen Datenschutz in **zwei Gesetzen** zu normieren. Eine solche Aufteilung macht Sinn,

- weil sich die *Rechtfertigungskonzepte* in den beiden Bereichen *entscheidend unterscheiden* (öffentlichrechtlich: Legalitätsprinzip / privatrechtlich: Einwilligung, überwiegendes Interesse, Gesetz), was (auch schon in der Vergangenheit) die Regulierung in den allgemeinen Grundsätzen (für beide Bereiche) und besonderen Bestimmungen (je für einen Bereich) kompliziert und schwerfällig macht, und
- weil wohl nur damit die *Frist* zur Umsetzung der schengenrelevanten Richtlinie (EU) 2016/680 eingehalten werden kann.

privatim
die schweizerischen datenschutzbeauftragten
les préposé(e)s suisses à la protection des données
gli incaricati svizzeri della protezione dei dati
c/o Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 2015, CH-4010 Basel
Tel. +41 (61) 201 16 40, Fax +41 (61) 201 16 41

Ausserdem könnten damit für die Zukunft **zwei Handlungsoptionen offengehalten** werden:

- Einerseits könnten mittelfristig – wie in vielen Kantonen mit dem Öffentlichkeitsprinzip – die Regelung des *Datenschutzes und* des *Öffentlichkeitsprinzips* als zwei Seiten derselben Medaille *in einem Gesetz* zusammengeführt werden.
- Andererseits könnte längerfristig, nachdem dafür die notwendige Verfassungsgrundlage geschaffen worden ist, ein *einheitliches, schweizweit geltendes Datenschutzgesetz für alle öffentlichen Organe* geschaffen werden. Damit müssten auch nicht mehr bei jeder Änderung des übergeordneten internationalen Rechts das Bundesdatenschutzgesetz und 26 kantonale Datenschutzgesetz angepasst werden, was erfahrungsgemäss (wie auch dieses Mal) zeitlich äusserst anspruchsvoll ist, weil die Kantone faktisch abwarten müssen, wie der Bund die geforderten Anpassungen umsetzt.

Stärkung des präventiven Datenschutzes

Das VE-DSG will den präventiven Datenschutz stärken. Hierzu sind aber die *notwendigen Instrumente konsequenter umzusetzen* – insbesondere in den folgenden Bereichen:

Datenschutz-Folgenabschätzung und Vorabkonsultation (Art. 16 VE-DSG)

Die Datenschutz-Folgenabschätzung (Art. 16 Abs. 1 und 2 VE-DSG) und die Vorabkonsultation (Art. 16 Abs. 3 und 4 VE-DSG) sind in zwei separaten Artikeln zu regeln. Das Instrument der *Vorabkonsultation* ist (mindestens bei Datenbearbeitungen von Bundesorganen) *obligatorisch* zu erklären, wenn diese zu einem erhöhten Risiko für die Persönlichkeit oder für die Grundrechte der betroffenen Personen führen.

Eine **Datenschutz-Folgenabschätzung** hat *bei jedem Vorhaben einer Datenbearbeitung* stattzufinden. Was im VE-DSG als Voraussetzung formuliert wird («voraussichtlich zu einem erhöhten Risiko führt»), ist bereits das Resultat eines ersten Schrittes der Folgenabschätzung. Diese Datenschutz-Folgenabschätzung ist im Grunde genommen nichts anderes als die Vorbereitung des Verantwortlichen, damit er die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften (Art. 19 lit. a VE-DSG) erbringen kann. Ausserdem beschlägt sie dieselben Punkte, die bei Vorhaben, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, für eine Vorabkonsultation (Art. 16 Abs. 3 und 4 VE-DSG) erarbeitet werden müssen.

Die **Vorabkonsultation**, wie sie von Art. 8bis Ziff. 2 des Übereinkommens SEV 108 und von Art. 28 der Richtlinie (EU) 2016/680 verlangt wird, wird in Art. 16 Abs. 3 und 4 VE-DSG ungenügend umgesetzt. Die Vorabkonsultation (oder Vorabkontrolle, wie sie bei den bisher geltenden europarechtlichen Vorgaben hiess) hätte vom Bund bereits bei der Schengen-Assoziierung eingeführt werden müssen. Sie ist eines der *wirksamsten Mittel des präventiven Datenschutzes*, wie die verbreitete Praxis bei den Kantonen beweist.

Wenn die Datenschutz-Folgenabschätzung ein erhöhtes Risiko für die Persönlichkeit (bei privatrechtlichem Datenbearbeiten) oder für die Grundrechte der betroffenen Personen (bei öffentlich-rechtlichem Datenbearbeiten) ergibt, soll das Ergebnis zusammen mit den vorgesehenen Massnahmen – mindestens bei Vorhaben der Bundesorgane – *zwingend dem Beauftragten zur Vorabkonsultation* vorgelegt werden. Er hat dann zu prüfen, ob die Verantwortlichen die Risiken für die Grundrechte der betroffenen Personen nicht hinrei-

chend ermittelt oder durch die vorgeschlagenen Massnahmen nicht hinreichend eingedämmt haben.

«Datenschutz durch Technik»: Privacy by Design, Privacy by Default (Art. 18 VE-DSG)

Aus der Formulierung von Art. 18 Abs. 1 VE-DSG wird nicht klar, wie weit hier eine Verpflichtung der Verantwortlichen entstehen soll, die nicht bereits aufgrund von Art. 11 VE-DSG besteht. *Fragwürdig* erscheint deshalb auch die mögliche *strafrechtliche Sanktionierung der Unterlassung von Massnahmen* gemäss Art. 18 VE-DSG (Art. 51 Abs. 1 lit. e VE-DSG). **«Datenschutz durch Technik»** ist eine mögliche Massnahme aufgrund der Vorgaben von Art. 11 VE-DSG und daher Teil eines gesamten Massnahmenpakets gestützt auf Art. 11 VE-DSG. Abs. 1 ist deshalb mit Art. 11 VE-DSG zusammenzuführen.

Wie bereits in den Erläuterungen angetönt, ist Art. 18 Abs. 2 VE-DSG nur für den privatrechtlichen Teil sinnvoll, da Bundesorgane Daten nur aufgrund einer Rechtsgrundlage bearbeiten (Art. 27 VE-DSG). Die Formulierung ist deshalb entsprechend anzupassen. Zudem könnte Abs. 2 auch in Zusammenhang mit Art. 4 VE-DSG eingeordnet werden.

Stärkung der Wirkung des Gesetzes und der Rechte der betroffenen Personen

Im Zentrum der Totalrevision des DSG steht die *Stärkung der Wirkung des Gesetzes und der Rechte der betroffenen Personen*. In Bezug auf die Stärkung der Rechte der betroffenen Personen werden indessen zwei zentrale Elemente der EU-Reform ignoriert: Art. 20 Verordnung (EU) 2016/679 sieht ein **Recht auf Datenübertragbarkeit** vor und Art. 17 Verordnung (EU) 2016/679 ein **Recht auf Löschung («Recht auf Vergessenwerden»)**. Beide Rechte stärken die Position der betroffenen Personen insbesondere gegenüber grossen global tätigen Datenbearbeitern. Es ist nicht nachzuvollziehen, warum den Schweizer Bürgerinnen und Bürger ein solches Recht verwehrt werden soll. privatim empfiehlt deshalb, die Aufnahme dieser beiden Rechtsinstrumente in die Totalrevision des DSG ernsthaft zu prüfen.

Die Zivilprozessordnung (ZPO) soll dahingehend geändert werden, dass für Klagen und Begehren nach dem Datenschutzgesetz keine Sicherheiten zu leisten und keine Gerichtskosten zu bezahlen sind. Diese Erleichterungen in der Prozessführung für die betroffene Person können für sich die Schwelle für die Durchsetzung der eigenen Rechte nicht herabsetzen. Die in den Erläuterungen aufgrund des Fehlens von wirkungsvollen Rechtsdurchsetzungsinstrumenten vor allem im privaten Sektor festgestellte erheblich verringerte Wirksamkeit des Datenschutzgesetzes kann nur aufgefangen werden, wenn neben den Kosten auch die Beweisführung für die betroffene Person erleichtert wird. privatim empfiehlt deshalb für Verfahren aufgrund des Datenschutzgesetzes eine **Beweislastumkehr**, da es der betroffenen Person aufgrund der Komplexität der heutigen Datenbearbeitungen in vielen Fällen gar nicht möglich ist, den Beweis für das unbefugte Bearbeiten zu erbringen. Dies bedeutet auch keine zusätzliche Belastung des Verantwortlichen, da dieser den *Nachweis der Konformität seiner Datenbearbeitungen* auch unabhängig von einem Verfahren zu dokumentieren hat (Art. 19 lit. a VE-DSG).

Verwaltungssanktionen: keine Abwälzung auf das Strafrecht

privatim lehnt den Ausbau der Strafbestimmungen im VE-DSG ab (Art. 50 ff. VE-DSG). Mit den vorgesehenen Strafbestimmungen werden bisherige Vollzugsdefizite des DSG

auf das Strafrecht abgewälzt. Bereits die bestehenden Strafbestimmungen des DSG haben sich in Bezug auf eine einheitliche Vollstreckung des DSG nicht bewährt. Strafurteile aufgrund der Strafbestimmungen des DSG sind fast gänzlich unbekannt. Mit den neuen Bestimmungen tritt der Strafrichter in Konkurrenz zur Datenschutzaufsichtsbehörde, was weder institutionell noch sachlich sinnvoll ist. Zahlreichen der neuen Strafbestimmungen fehlt die Bestimmtheit, so dass sie dem Grundsatz «Nulla poena sine lege» widersprechen. Zudem werden mit den umschriebenen Strafbestimmungen die Vorgaben gemäss Richtlinie (EU) 2016/680 und Art. 12bis Abs. 2 lit. c E-SEV 108 nicht vollständig umgesetzt. Die EU sowie der Europarat verlangen ausdrücklich auch **Verwaltungssanktionen**, die der Beauftragte verhängen kann. Die angedrohten strafrechtlichen Sanktionen von max. 500'000 CHF wirken keinesfalls abschreckend und sind im Vergleich zu den Sanktionsmöglichkeiten nach dem EU-Recht für global tätige Unternehmen bedeutungslos. Mit den Strafbestimmungen wird die Strafverfolgung zudem an die Kantone delegiert. Damit müssen die Kantone nicht nur ressourcenmässig für den Vollzug des VE-DSG aufkommen, sondern es ist aufgrund der spezifischen Materie des Datenschutzrechts auch damit zu rechnen, dass *kein einheitlicher Vollzug möglich* sein wird. Der Vollzug und die Sanktionierung von Verstössen gegen das VE-DSG sind aus Sicht von privatim eine Bundesaufgabe und somit durch den Bund wahrzunehmen.

Ressourcen des EDÖB

Das VE-DSG enthält erweiterte Kompetenzen und Aufgaben für den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Dies wird nur mit einem **wesentlichen Ausbau der Ressourcen des EDÖB** möglich sein. Werden diese Ressourcen nicht zugeteilt, kann ebenso auf den Ausbau der Kompetenzen und Aufgaben verzichtet werden. Gestützt auf Art. 43 VE-DSG wird dem Beauftragten lediglich die Möglichkeit von Verwaltungsmassnahmen gegeben. Allerdings verlangen die europarechtlichen Vorgaben (Art. 12bis Abs. 2 lit. c E-SEV 108) wirksame, verhältnismässige und abschreckende Sanktionsmöglichkeiten. Gemäss dem Erläuternden Bericht soll dies ohne Sanktionsmöglichkeiten des Beauftragten lediglich durch die erweiterten Strafbestimmungen des VE-DSG erfolgen. Der erweiterte Einbezug des Strafrechts in den Vollzug des Datenschutzrechts ist aber – wie bereits gesehen – ein untauglicher Weg, die europarechtlichen Vorgaben zu erfüllen. Der Beauftragte muss deshalb zusätzlich bei Verstössen gegen das Datenschutzrecht auch *administrative Sanktionen* verhängen können (etwa Bussen), und zwar mindestens gegenüber Privaten. Art. 43 VE-DSG ist entsprechend zu ergänzen. Die Organisation des EDÖB ist deshalb allenfalls analog der Wettbewerbskommission auszubauen[1].

Spezifische Bestimmungen

Geltungsbereich (Art. 2 VE-DSG)

Der Ausschluss der Rechtsprechung aus dem Geltungsbereich des DSG entspricht nicht dem Übereinkommen SEV 108, das keine Möglichkeiten zur Ausnahme vom Geltungsbereich vorsieht. privatim schlägt deshalb folgende Regelung vor: *Geltung des DSG* (d. h. der Grundsätze, z. B. betreffend Informationssicherheit, Vorabkonsultation usw.) *auch für*

[1] Vgl. Erläuternder Bericht zum VE-DSG vom 21. Dezember 2016, S. 83.

die Rechtsprechungsorgane. Die Prozessordnungen gelten als bereichsspezifisches Datenschutzrecht (d. h. lex specialis) ohnehin[2].

Einzig zwei Ausnahmen sind erforderlich (und konventionskonform) – sie werden auch von der Konferenz der Kantonsregierungen in ihrem Leitfaden für die Anpassung der kantonalen Datenschutzgesetze so empfohlen:

Damit nicht die Rechte der betroffenen Personen und die Parteirechte der Prozessordnungen kollidieren, kann (in Art. 2 VE-DSG) festgelegt werden, dass sich während der Hängigkeit eines gerichtlichen Verfahren die Ansprüche und Rechte der betroffenen Personen ausschliesslich nach dem anwendbaren Verfahrensrecht richten, so dass in dieser Phase die Parteien z. B. nur ihr verfahrensrechtliches Akteneinsichtsrecht geltend machen können, nicht aber ihr datenschutzrechtliches Recht auf Auskunft (auf Zugang zu den eigenen Personendaten).

Damit nicht Aufsichtsrechte/-pflichten kollidieren, kann (z. B. in Art. 40 VE-DSG) festgelegt werden, dass die Datenbearbeitungen in hängigen gerichtlichen Verfahren vor eidgenössischen Gerichten von der Aufsicht durch den EDÖB ausgenommen sind.

Begriffe (Art. 3 VE-DSG)

privatim begrüsst die Aufnahme des *Kriteriums «Ethnie»* (Zugehörigkeit zu einer Gruppe von Menschen, die sich aufgrund ihrer Kultur, Geschichte, Sprache, Sitten, Traditionen und Gebräuche als untereinander verbunden und dadurch als von der übrigen Bevölkerung differente Gemeinschaft erleben und/oder von der übrigen Bevölkerung als differente Gruppe wahrgenommen werden).

Demgegenüber beantragt privatim die *Streichung des Begriffs «Rasse».* «Rasse» ist in Bezug auf die Menschen kein wissenschaftlicher Begriff; geschützt werden soll vielmehr vor dem Rassevorwurf (historisch: «Jude», «Neger» usw.).

Ebenfalls begrüsst wird die Aufnahme des *Begriffs «genetische Daten»* in die besonders schützenswerten Personendaten.

Der *Begriff der «biometrischen Daten»* hingegen ist missverständlich. Auch in den Erläuterungen wird er nicht geklärt: Ein Gesichtsbild (ein Portrait) ist grundsätzlich auch ein «biometrisches Datum», soll aber hier nicht als Unterkategorie der besonders schützenswerten Personendaten erfasst werden. Deshalb ist, wie dies auch die Konferenz der Kantonsregierungen in ihrem Leitfaden für die Anpassung der kantonalen Datenschutzgesetze tut, die *folgende Definition* aufzunehmen:

> *«4. mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Peron ermöglichen oder bestätigen (biometrische Daten)».*

Der *Begriff «Speichern»* widerspricht dem Anliegen der technikneutralen Formulierung des Gesetzes.

---

[2] Vgl. dazu BEAT RUDIN, Überholte Ausnahmen im Geltungsbereich, digma 2016, S. 122 ff.

In der Vernehmlassungsvorlage (Art. 4 Abs. 5, Art. 25 Abs. 1, Art. 29 und 30 VE-DSG) und auch in der Richtlinie (EU) 2016/680 werden die *Begriffe «Löschen» und «Vernichten»* nebeneinander verwendet, ohne dass das Verhältnis der beiden zueinander geklärt wird. Vernichten hat bisher das endgültige physische «Zerstören» gemeint. Ob Löschen nur das «Entfernen aus dem aktiven Prozess» (ähnlich wie das Löschen von Strafregistereinträgen) meint oder einfach das Vernichten im elektronischen Umfeld umschreibt, muss festgelegt werden. Dies ist deshalb im Gesetzestext oder mindestens im Botschaftstext zu klären.

privatim begrüsst den *Ersatz des* bis heute unklaren *Begriffs des «Persönlichkeitsprofils»* (als «gefährliche» Art von Daten) *durch das «Profiling»* (als «gefährliche» Art des Bearbeitens von Daten). Allerdings ist es völlig *ungenügend*, wenn dann im bereichsspezifischen Datenschutzrecht (in den anzupassenden Bundesgesetzen) mit *Blankettermächtigungen* das Profiling quasi «durchgewinkt» wird. Verlangt ist, dass klare und strenge Rahmenbedingungen für das Profiling in den Bundesgesetzen konkretisiert werden.

Im schweizerischen Recht sollte vom «Auftrags*daten*bearbeiter» gesprochen werden: Diese Person/Stelle muss nicht einfach einen Auftrag bearbeiten, sondern im Auftrag des Verantwortlichen Daten bearbeiten. Eine Abweichung vom Begriff im europäischen Recht ist problemlos möglich, da mit dem Bearbeiter (anstelle des Verarbeiters) ohnehin schon – und zu Recht – von der europäischen Begrifflichkeit abgewichen wird. Ausserdem verwendet der VE-DSG den Begriff der Auftragsdatenbearbeitung auch schon in der Überschrift von Art. 7.

Begrüsst wird auch die Streichung des Begriffs der «Datensammlung», da dieser Begriff im Zeitalter der Digitalisierung völlig veraltet ist und an etwas anknüpft, das im modernen IT-Umfeld längst nicht mehr gegeben ist.

Grundsätze (Art. 4 VE-DSG)

privatim begrüsst die Neuformulierung und Ergänzungen von Art. 4 DSG. Zu Art. 4 Abs. 4 VE-DSG ist festzustellen, dass die *Festlegung von Aufbewahrungsfristen* impliziert wird. Diese Pflicht der Verantwortlichen sollte mindestens im Botschaftstext zum Ausdruck kommen.

Es ist zu begrüssen, dass bei der *Einwilligung* festgehalten wird, dass sie nicht nur freiwillig, sondern auch eindeutig zu erfolgen hat. Im zweiten Satz sollte aber auch der Begriff «ausdrücklich», dessen Bedeutung bisher in der Literatur kontrovers diskutiert wurde, mindestens durch eine Erläuterung im Botschaftstext geklärt werden.

Auftragsdatenbearbeitung (Art. 7 VE-DSG)

Die Bestimmung übernimmt weitgehend die Formulierung von Art. 10*a* DSG. Allerdings kommen dadurch die europarechtlichen Vorgaben (insbesondere aus der Richtlinie (Art. 22 f. RL (EU) 2016/680) für die Bundesorgane) nicht korrekt zum Ausdruck. In Bezug auf die Begriffe sollte analog zur Überschrift auch im Text vom Auftrags*daten*bearbeiter gesprochen werden.

Der Verantwortliche muss sich nicht nur vergewissern, dass die Datensicherheit und die Rechte der betroffenen Personen gewährleistet sind, sondern er *muss wirksam sicherstel-*

len, dass die Daten nur so bearbeitet werden, wie der Verantwortliche es selber tun darf. Entsprechend ist die Formulierung in lit. a zu ergänzen.

Art. 7 Abs. 2 VE-DSG ist in Abhängigkeit von der Anpassung in lit. a neu zu formulieren. Zudem sollte der Bundesrat nicht Anforderungen an den Auftragsdatenbearbeiter präzisieren, sondern die *Verantwortlichen in die Pflicht nehmen*, indem die einzelnen Anforderungen an die Auswahl des Dritten und die Sicherstellung, dass die Personendaten nur so bearbeitet werden, wie es der Verantwortliche tun dürfte, auf Verordnungsstufe detailliert geregelt werden.

Empfehlungen der guten Praxis (Art. 8 und 9 VE-DSG)

Das neue Instrument der Empfehlungen der guten Praxis, wobei der Beauftragte solche zu erarbeiten oder zu genehmigen hat, ist kritisch zu beurteilen. Dieses Instrument braucht *bedeutende Ressourcen*, um zum richtigen Zeitpunkt zusammen mit den interessierten Kreisen und unter Berücksichtigung der Besonderheiten eines Anwendungsbereichs über Empfehlungen zu verfügen, die in der Praxis auch Wirkung erzielen können. Solange nicht geklärt ist, wie diese Ressourcen dem Beauftragten zur Verfügung gestellt werden, erscheint dieses Instrument als wirkungslos.

Es ist zu präzisieren, dass die Konkretisierung durch die Empfehlungen der guten Praxis die *Datenschutzvorschriften des Bundesrechts* betrifft. Sofern Empfehlungen der guten Praxis auch den öffentlich-rechtlichen Bereich betreffen sollen, ist ihre Anwendbarkeit auf die Bundesorgane zu beschränken oder allenfalls eine Zusammenarbeit mit den kantonalen Datenschutzaufsichtsbehörden zu suchen. Dies sollte mindestens im Botschaftstext präzisiert werden.

Der Wortlaut von Art. 9 VE-DSG bringt zu wenig zum Ausdruck, dass es sich bei der Einhaltung der Empfehlungen der guten Praxis lediglich um eine *gesetzliche Vermutung der Einhaltung der Datenschutzvorschriften* handelt. Da es sich aber generell bei den Empfehlungen der guten Praxis um eine Konkretisierung des Gesetzes handeln soll und die Empfehlungen nie die Konkretisierung des gesamten Gesetzes umfassen können, trägt diese gesetzliche Vermutung auch nur einen Teil zur Gesamtbeurteilung bei, ob eine Datenbearbeitung die Datenschutzvorschriften einhält. Dies wird auch dadurch unterstrichen, dass die Einhaltung der Empfehlungen der guten Praxis freiwillig ist (Abs. 2). Aus diesem Grund könnte Art. 9 VE-DSG ersatzlos gestrichen werden, ohne dass dies die Wirkung des Gesetzes beeinträchtigen würde.

Zertifizierung (Art. 10 VE-DSG)

In den Erläuterungen zu Art. 10 VE-DSG wird darauf verwiesen, dass keine Änderungen zum bisherigen Art. 11 DSG bestehen, obwohl Art. 10 VE-DSG nur noch von «Datenbearbeitungsvorgängen» spricht, im Gegensatz zu Art. 11 DSG, der auch die «Datenbearbeitungssysteme und -programme» (Produkte) explizit erwähnt. Diese Änderung des Wortlauts deckt sich nicht mit den Erläuterungen, die davon ausgehen, dass die Produkte auch mitenthalten seien. Dabei ist in Art. 10 VE-DSG die Zertifizierung nur noch für Verantwortliche oder Auftragsdatenbearbeiter möglich, was gerade die Hersteller von Produkten ausschliesst. Da die Produktezertifizierung auch nach dem bisherigen Recht toter Buchstabe geblieben ist, kann sie durchaus ausgeschlossen werden, was aber zumindest im Botschaftstext klar festzuhalten wäre.

Sicherheit von Personendaten (Art. 11 VE-DSG)

Art. 11 VE-DSG orientiert sich zu stark am bisherigen Art. 7 DSG und unterlässt es, Schutzziele zu definieren wie dies Art. 32 Abs. 1 lit. b Verordnung (EU) 2016/679 und Art. 29 Abs. 2 Richtlinie (EU) 2016/680 tun, und wie sie auch in modernen kantonalen Datenschutzgesetzen zu finden sind (z. B.: § 7 IDG/ZH, § 8 IDG/BS). Dabei ist auch der veraltete Begriff des «unbefugten Bearbeitens» zu hinterfragen. Zudem sind Massnahmen gegen das «unbefugte Bearbeiten» *und* den «Verlust» zu treffen (das «oder» als Alternative wäre falsch). privatim schlägt deshalb vor, die *Schutzziele explizit im Gesetz zu erwähnen*.

Daten einer verstorbenen Person (Art. 12 VE-DSG)

Wir begrüssen grundsätzlich, dass eine Regelung für den Zugang zu Daten einer verstorbenen Person vorgesehen wird. Allerdings hat privatim *Zweifel*, ob die vorgeschlagene Lösung der Sachlage gerecht wird.

Eine Untersagung i.S.v. Art. 12 Abs. 1 lit. a VE-DSG wird im Alltag kaum je vorkommen. Somit hängt die Entscheidung allein an einer Interessenabwägung nach Art. 12 Abs. 1 lit. b VE-DSG, allerdings mit der Schwierigkeit, dass die abzuwägenden Interessen der verstorbenen Person durch den Datenbearbeiter, der Einsicht geben soll, schwer zu ermitteln und zu gewichten sind (wenn man nicht davon ausgeht, dass mit dem Tod die Interessen der verstorbenen Person ohnehin «untergehen»). Es ist deshalb zu prüfen, ob die Norm nicht restriktiver ausgestaltet werden muss.

Die *Ausschaltung der Amtsgeheimnisse* (insbesondere der besonderen Amtsgeheimnisse, also nicht bloss der personalrechtlichen Pflicht zur Verschwiegenheit) *und der Berufsgeheimnisse* einzig aufgrund einer Interessenabwägung (Art. 12 Abs. 1 VE-DSG) erscheint *äusserst problematisch*. Der Weg, aus solchen Schweigeverpflichtungen «herauszukommen», ist die Entbindung durch die Aufsichtsbehörde. Dieser Absatz ist deshalb zu streichen oder restriktiver zu formulieren.

Automatisierte Einzelentscheidungen (Art. 15 VE-DSG)

Von Bedeutung ist diese Regelung vor allem im *Privatrecht*. Für diesen Bereich wird sie begrüsst.

Im öffentlichen Recht ergehen Einzelentscheidungen mit rechtlichen Wirkungen in aller Regel in Form der Verfügung. Weil diese eröffnet werden müssen, ist die Information der betroffenen Personen sichergestellt. Weil den betroffenen Personen im Vorfeld des Erlasses von Verfügungen ein Anspruch auf rechtliches Gehör zukommt, ist auch sichergestellt, dass sie sich zur Einzelentscheidung äussern können. Aus diesem Grund geht der KdK-Leitfaden für die Umsetzung in den kantonalen DSG davon aus, dass es keine spezifische Regelung in den kantonalen (Informations- und) Datenschutzgesetzen braucht. Zum einen ist deshalb die Regelung (ohne Abs. 3) in den Abschnitt zum Datenbearbeiten durch Private zu verschieben. Zum andern sind *im öffentlich-rechtlichen Bereich* automatisierte Einzelentscheidungen, die nicht in Form einer Verfügung eröffnet werden, ausschliesslich zuzulassen, wenn ein *Gesetz (im formellen Sinn)* dies *ausdrücklich* vorsieht und das Gesetz gleichzeitig *geeignete Massnahmen zum Schutz der Rechte der betroffe-*

nen Personen (insbesondere bezüglich der Transparenz und Einwirkungsmöglichkeiten für die betroffenen Personen) vorsieht.

Meldepflicht bei Datenschutzverletzungen (Art. 17 VE-DSG)

Die «Verletzung des Datenschutzes» wird in Art. 17 Abs. 1 VE-DSG nicht klar definiert, was aber auch im Hinblick auf die mögliche Strafbarkeit des Verantwortlichen (siehe Art. 50 Abs. 2 lit. e und Art. 50 Abs. 3 lit. b VE-DSG) unentbehrlich ist. Die Definition ist entweder in diesem Artikel oder unter den Begriffen (Art. 3 VE-DSG) nachzutragen. Dabei schlägt privatim vor, die *Definition* gemäss dem KdK-Leitfaden für die Umsetzung in den kantonalen DSG zu formulieren:

> *«Eine Datenschutzverletzung liegt vor, wenn die Sicherheit so verletzt wird, dass bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten.»*

Die Meldepflicht soll entfallen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt. Diese Formulierung lässt dem Verantwortlichen einen weiten Ermessensspielraum, der faktisch die vorsätzliche oder fahrlässige Strafbarkeit der Nichtmeldung ausschliesst. Der Ermessensspielraum ist deshalb konkreter einzuschränken und die Anwendung des Strafrechts zu überdenken.

Weitere Pflichten (Art. 19 VE-DSG)

Entgegen den Ausführungen in den Erläuterungen, ist festzuhalten, dass die in Art. 19 lit. a VE-DSG statuierte *Dokumentationspflicht* den Anforderungen von Art. 8^{bis} Ziff. 1 E-Übereinkommen SEV 108 und Art. 4 Abs. 4 RL 2016/680 nicht entspricht. Vielmehr müssen der Verantwortliche und der Auftragsdatenbearbeiter nachweisen können, dass sie die Datenschutzbestimmungen einhalten. Dies geht über ein Register der Datenbearbeitungen hinaus.

Dieser Nachweis kann in einem *Datenschutzmanagementsystem* (DSMS) erbracht werden. DSMS basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Wird auf eine diesbezügliche Zertifizierung verzichtet, ist festzulegen, welche Dokumente notwendig sind, um diesen Nachweis erbringen zu können (z. B. Informationssicherheitskonzept, Zugriffskonzept usw.). Hierzu bestehen bereits zahlreiche Hilfsmittel.

Es ist sinnvollerweise auf Verordnungsstufe festzulegen, in welchen Fällen ein solches DSMS obligatorisch sein soll (z. B. nur, wenn besonders schützenswerte Personendaten bearbeitet werden).

Eine klare Regelung ist zudem erforderlich, da das Fehlen einer Dokumentation strafrechtlich sanktioniert werden soll (Art. 51 Abs. 1 lit. f VE-DSG), was nur bei einer genügenden Bestimmtheit der Strafnorm möglich ist.

Auskunftsrecht (Art. 20 VE-DSG)

Wir begrüssen, dass ausdrücklich festgehalten wird, dass die Auskunft über die eigenen Personendaten (der «Zugang zu den eigenen Personendaten») als Inbegriff der Ausübung des Grundrechts auf informationelle Selbstbestimmung *kostenlos* zu gewähren ist, und dass auf Gesetzesstufe ausdrücklich festgehalten wird, welche Informationen mitgeteilt werden müssen.

Persönlichkeitsverletzungen (Art. 23 VE-DSG)

Es ist nicht sinnvoll, beim Profiling eine tatbestandsausschliessende Einwilligung vorzusehen. Ein Profiling im Sinne der Legaldefinition (siehe Ergänzung zu Art. 3 lit. f VE-DSG) stellt eine Persönlichkeitsverletzung dar. Sie kann aber, wie in Art. 24 Abs. 1 VE-DSG vorgesehen, durch eine Einwilligung der betroffenen Person gerechtfertigt werden – in Verbindung mit der Regelung von Art. 4 Abs. 6 VE-DSG ist klar, dass bei einem Profiling die Einwilligung ausdrücklich erteilt werden muss. Die Worte *«ohne ausdrückliche Einwilligung der betroffenen Person» sind deshalb zu streichen*.

Rechtfertigungsgründe (Art. 24 VE-DSG)

Nach dem geltenden Recht waren Datenbearbeitungen durch Wirtschaftsinformationsunternehmen (Wirtschaftsauskunfteien) durch ein überwiegendes Interesse gerechtfertigt, solange diese keine Persönlichkeitsprofile bearbeiteten. Im VE-DSG wird das Persönlichkeitsprofil (als «gefährliche» Datenart) ersetzt durch das Profiling (als «gefährliche» Art der Datenbearbeitung). Im nun vorgeschlagenen Art. 24 Abs. 2 lit. c VE-DSG wird das Profiling erlaubt, ohne dass – ausser dem Erfordernis der Volljährigkeit der betroffenen Personen (Ziff. 3) – in irgendeiner Weise strengere Anforderungen an das Profiling gestellt werden. Dies ist zu überprüfen, und es sind *strengere Anforderungen an das Profiling durch Wirtschaftsinformationsunternehmen* zu stellen.

Rechtsgrundlagen (Art. 27 VE-DSG)

Beim Profiling müssen im Gesetz geeignete Garantien zum Schutz der Grundrechte der betroffenen Personen vorgesehen sein. Blankettnormen (wie etwa: «das Bundesamt darf besondere Personendaten bearbeiten und ein Profiling durchführen») reichen keinesfalls.

Es ist deshalb zu verdeutlichen, dass aus diesem Grund ein *Profiling immer eine Grundlage in einem formellen Gesetz voraussetzt*, weil ein Profiling immer besondere Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen birgt und deshalb nach Art. 27 Abs. 2 lit. b VE-DSG nicht auf Grundlage einer Regelung in einem Gesetz im materiellen Sinn zulässig ist.

Untersuchung (Art. 41 VE-DSG)

Es ist zu begrüssen, dass dem Beauftragten *erweiterte Untersuchungsbefugnisse* zugestanden werden. Dies entspricht den Vorgaben des E-SEV 108 (Art. 12^{bis} Ziff. 3) sowie der Richtlinie (EU) 2016/680 (Art. 52). Allerdings stellen diese Vorgaben klar, dass der Beauftragte nicht die Wahl hat, ob er auf eine Anzeige einer betroffenen Person reagieren will oder nicht («kann»), da er diesbezüglich klarerweise eine *Behandlungspflicht* hat. Dies müsste im Gesetzestext im Verhältnis zu Art. 41 Abs. 5 VE-DSG besser zum Ausdruck

gebracht werden. Es ist deshalb auch davon auszugehen, dass dem Beauftragte für diese Aufgabenerfüllung *erheblich mehr Ressourcen* zur Verfügung stehen müssen als die derzeit in den Erläuterungen erwähnten «maximal ein oder zwei Stellen»[3].

Art. 41 Abs. 5 VE-DSG ist zu unspezifisch formuliert. Obwohl nicht davon auszugehen ist, dass dem Beauftragten eine eigentliche Untersuchungspflicht obliegt, so ist doch klarerweise von einer Behandlungspflicht auszugehen. Es dürfte sich hier in Umsetzung von Art. 52 und 53 Richtlinie (EU) 2016/680 verwaltungsrechtlich wohl um eine «Aufsichtsbeschwerde» *(«aufsichtsrechtliche Anzeige»)* handeln. Entsprechend ist der Beauftragte *verpflichtet*, sich mit dieser Anzeige zu *befassen*. Art. 41 Abs. 5 VE-DSG ist verbindlicher umzuformulieren. Zusätzlich sollte noch die Behandlungsfrist von drei Monaten erwähnt werden. Zumindest müsste diesbezüglich der Botschaftstext Klarheit schaffen.

Vollzug durch die Kantone (Art. 57 VE-DSG)

Dieser Artikel ist zu *streichen*. Seit dem Beitritt der Schweiz zum Schengenraum (Schengener-Assoziierungsabkommen) resp. spätestens mit der Umsetzung der neuen Richtlinie (EU) 2016/680 und bei Ratifizierung des revidierten Übereinkommens SEV 108 sind auch die Kantone verpflichtet, einen angemessenen Schutz von Personendaten durch unabhängige Datenschutzaufsichtsbehörden zu gewährleisten. Diese «Auffangnorm» ist daher obsolet.

[3] Vgl. Erläuternder Bericht zum VE-DSG vom 21. Dezember 2016, S. 109.