EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Bundesamt für Justiz
Direktionsbereich öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

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

Zürich, 3. April 2017

Stellungnahme zur Vernehmlassung zum Entwurf des Bundesgesetzes über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Bundesrat hat das Eidg. Justiz- und Polizeidepartement (EJPD) am 21. Dezember 2016 beauftragt, bei den interessierten Kreisen zum Entwurf des Bundesgesetzes über den Datenschutz ein Vernehmlassungsverfahren durchzuführen.

Gemäss der Medienmitteilung vom 21. Dezember 2016 will der Bundesrat primär die jüngsten Entwicklungen im Bereich des Datenschutzes in der EU und beim Europarat berücksichtigen sowie mit der Revision die Grundlage dafür schaffen, dass die Schweiz die Datenschutzkonvention des Europarates ratifizieren und die EU-Richtlinie über den Datenschutz im Bereich der Strafverfolgung übernehmen kann. Damit soll sichergestellt sein, dass die grenzüberschreitende Datenübermittlung weiterhin möglich bleibt. Zudem soll die Transparenz bei der Datenbearbeitung erhöht werden, Informationspflichten der Datenbearbeiter ausgeweitet, das Auskunftsrecht der betroffenen Personen präzisiert und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) mehr Kompetenzen verliehen werden. Überdies sollen die Strafbestimmungen verschärft werden.

Gerne nehmen wir zum Vorentwurf Datenschutzgesetz (VE-DSG) wie folgt Stellung:

Auch wir sind der Ansicht, dass das neue Datenschutzrecht der Schweiz den Vorgaben auf EU- und Europarats-Ebene möglichst entsprechen muss. In der VE-DSG sind nun aber verschiedene Regelungen enthalten, die über das Ziel hinausschiessen sowie für die in der Schweiz tätigen Unternehmen zu einem unnötigen administrativen und finanziellen Aufwand und – insbesondere für die international tätigen Unternehmen – zu einem Standortnachteil führen würden.

EXPERTsuisse – Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand
Limmatquai 120, Postfach, CH-8021 Zürich, Tel. +41 58 206 05 05, Fax +41 58 206 05 09
info@expertsuisse.ch, www.expertsuisse.ch

Die Totalrevision des Datenschutzgesetzes in der Schweiz darf keinesfalls zur Folge haben, dass der Datentransfer bei grenzüberschreitenden Tätigkeiten der international tätigen Unternehmen erschwert wird. Für die in der Schweiz ansässigen Revisionsgesellschaften, die für einen international tätigen Konzern eine Konzernprüfung durchführen, muss die Zulieferung von Datenmaterial zwischen der Muttergesellschaft und einer Tochtergesellschaft ohne grosse Einschränkung und Aufwand möglich sein.

Der Prüfer, der eine Teileinheit überprüft, ist auf diesen Datentransfer zwingend angewiesen. Es ist somit von grosser Wichtigkeit, dass die Möglichkeit, grenzüberschreitende Daten über verschiedene Kanäle auszutauschen, sichergestellt ist. Ferner ist zu erwarten, dass in ein paar Jahren ein massgebender Teil der Software in einer Cloud abgelegt sein wird. Der entsprechende Server würde dann in der Schweiz oder in der EU bzw. möglicherweise sogar einem Staat ausserhalb der EU liegen. Konzerne, die grenzüberschreitend tätig sind, würden ihre Daten in einer solchen Cloud ablegen.
In der EU-Datenschutz-Grundverordnung (EU-DSGVO) findet sich der Begriff *„Unternehmensgruppe“* (=herrschende(s) Unternehmen und von diesem abhängige Unternehmen). Art. 47 der DSGVO enthält eine Art **Konzernprivileg,** wonach gruppeninterne Datenweitergaben zwischen verbundenen Unternehmen unter erleichterten Voraussetzungen erfolgen. Mittels gruppeninternen vertraglichen Regelungen kann der Mindestinhalt des angemessenen Datenschutzniveaus festgesetzt werden. Es ist im Interesse des Wirtschaftsstandortes Schweiz, sicherzustellen, dass die Äquivalenz zur EU-Regelung gegeben und der grenzüberschreitende Datentransfer mit dem VE-DSG gewährleistet ist.

Mit Art. 52 VE-DSG soll der in Art. 321 StGB vorgesehene Schutz der beruflichen Schweigepflicht ausgebaut werden, da dieser durch die zunehmende Spezialisierung und die neuen Informationsbearbeitungsmethoden lückenhaft geworden sei (siehe Erläuternder Bericht). Gemäss Abs. 1 dieser Bestimmung wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (auf Antrag) bestraft, wer vorsätzlich geheime Daten bekannt gibt. Diese Bestimmung ist von überschiessender Tragweite. Es ist auch nicht wirklich eine Begründung für deren Notwendigkeit ersichtlich. Wohl ist klar, dass die erfolgreiche Ausübung der Berufe gemäss Art. 321 StGB ein besonderes Vertrauensverhältnis zum Klienten voraussetzt. Dementsprechend sind Verletzungen von Geheimhaltungspflichten zu sanktionieren. Alle anderen Berufe, bei welchen durchaus ein Geheimhaltungsbedürfnis besteht, sind aber nicht ohne weiteres gleichzusetzen mit den in Art. 321 StGB genannten. Datenschutzrechtlich ist insbesondere das Verhältnis zu Outsourcing-Konstellationen nicht genügend geklärt (gesetzliche und vertragliche Geheimhaltungspflichten verbieten ja ein Outsourcing ohne Einwilligung).

Für unsere Mitglieder bzw. die gesamte Branche ist das Revisionsgeheimnis eine der wichtigsten Pflichten, die es strikte einzuhalten gilt. Gemäss Art. 730b Abs. 2 OR muss die Revisionsstelle sowohl das Geheimnis über ihre Feststellungen wahren, soweit sie nicht von Gesetzes wegen zur Bekanntgabe verpflichtet ist. Sie wahrt auch die Geschäftsgeheimnisse der Gesellschaft bei der Berichterstattung, der Erstattung von Anzeigen und bei der Auskunftserteilung an die Generalversammlung. Die spezialgesetzlichen Prüfgesellschaften haben noch andere Gesetzesnormen (z.B. Art. 129 Abs. 1 KAG: Prüfgeheimnis) zu beachten. Ferner sei auf das verbandsrechtliche Berufsgeheimnis hingewiesen (vgl. Standes- und Berufsregeln von EXPERTsuisse). Die Pflicht zur *„unverzüglichen“* Meldung an den EDÖB (Art. 17 VE-DSG) birgt das Risiko, dass aus Angst vor der strengen Strafandrohung in Art. 50 Abs. 2 Bst. d VE-DSG vorschnell Informationen an den EDÖB weitergeleitet werden und dabei

(fahrlässig) ein Geschäftsgeheimnis/Berufsgeheimnis verletzt wird. Damit müssen die Unternehmen ihre Prozesse und Systeme deutlich ausbauen, was insbesondere für KMU einen unverhältnismässigen (finanziellen und organisatorischen) Aufwand zur Folge hätte.

Im Übrigen gibt es verschiedene Umsetzungsprobleme der geplanten Regelungen in der Praxis. Zu erwähnen ist beispielsweise das Recht der Betroffenen auf Löschung ihrer Daten. Daten können nur in *„live"*-Systemen gelöscht werden. Daten in einem Backup sind allerdings nicht mit einem vernünftigen Aufwand löschbar.

Wichtig ist auch, dass Innovationen und Entwicklungen in der digitalen Welt nicht durch das Datenschutzgesetz blockiert oder eingeschränkt werden sowie die Strategie des Bundesrates „Digitale Schweiz" im Fokus behalten wird.

Wir beantragen, dass diese Aspekte, insbesondere das Verhältnis zwischen Meldepflicht und Berufsgeheimnis nochmals einer genaueren Betrachtung zu unterziehen sind und bei der Totalrevision des DSG berücksichtigt werden.

Zum Entwurf des Datenschutzgesetzes stellen wir im Einzelnen folgende Hauptanträge:

1. Geltungsbereich

Gemäss dem VE-DSG soll das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren Anwendung finden, was bei den Auskunftsrechten zu Missbräuchen führen kann. Damit wird die Beweisbeschaffung über die zivilprozessualen Editionsrechte ausgehebelt. Der Geltungsbereich darf in dieser Hinsicht keinesfalls erweitert werden.

Wir beantragen, dass der Geltungsbereich des VE-DSG nicht auf rechtshängige Zivilprozesse und laufende Strafverfahren erweitert wird.

2. Wiederaufnahme Institut des internen Datenschutzbeauftragten

Wie erwartet, orientiert sich der VE-DSG sehr an der EU-DSGVO und es wurden zahlreiche Bestimmungen auf sehr ähnliche Weise übernommen. Es erstaunt daher umso mehr, dass ein wichtiges Element der EU-DSGVO nicht übernommen wurde, nämlich das Institut des betriebsinternen Datenschutzbeauftragten (vgl. Art. 11a Abs. 5 lit. 3 geltendes DSG). Dieser ist im VE-DSG nicht mehr vorgesehen. Weder der, ebenfalls am 21. Dezember 2016 veröffentlichte Erläuternde Bericht, noch eine Stellungnahme des Eidgenössischen Datenschutzbeauftragten erklärt die Löschung des entsprechenden Artikels. Die ersatzlose Streichung ist umso erstaunlicher, weil es sich beim internen Datenschutzbeauftragten um ein Kernelement der EU-DSGVO handelt. Die Streichung führt zu Unsicherheiten und kann u.E. auch zu Problemen im Hinblick auf die Diskussion der Gleichwertigkeit des Schweizerischen Datenschutzes mit demjenigen der EU führen.

Gerade im Hinblick darauf, dass eine grenzüberschreitende Datenübermittlung nach wie vor möglich ist, sollte diese Gleichwertigkeit mit dem aktuellen Vorentwurf angestrebt werden. Zumindest auf

freiwilliger Basis sollten die Unternehmen einen internen Datenschutzbeauftragten einführen können und damit von der Meldepflicht im Sinne von Art. 17 VE-DSG an den EDÖB entbunden sein, was insbesondere für grosse Unternehmen, die aufgrund ihres Gesellschaftszweckes viele Daten bearbeiten müssen, eine grosse Erleichterung wäre.

Wir beantragen die Beibehaltung des betriebsinternen Datenschutzbeauftragten, zumindest auf freiwilliger Basis, und unter gleichzeitiger Entbindung von der Mitteilungspflicht im Sinne von Art. 17 VE-DSG.

3. Begriffe (Art. 3 VE-DSG)

3.1. Bearbeiten

Die Begriffe *"Speichern"* und *"Löschen"* sind unnötig und daher zu löschen.

Wir beantragen die Streichung der Begriffe *„Speichern“* und *„Löschen“*.

3.2. Biometrische Daten (Art. 3 Bst. c Ziff. 3 und 4 VE-DSG)

Die Ausweitung des Begriffs *«besonders schützenswerte Personendaten»* auf genetische und biometrische Daten geht zu weit. Der Wortlaut widerspricht den Erläuterungen im Bericht: Angedacht war die Erfassung von Daten, welche zum Zweck bearbeitet werden, eine natürliche Person eindeutig zu identifizieren. Dies entspricht auch der Stossrichtung des Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (E-SEV 108). Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Wir beantragen, die Definition von Art. 3 Bst. c Ziff. 3 und 4 VE-DSG einzuschränken.

3.3. Profiling (Art. 3 Bst. f VE-DSG)

Der Verzicht auf den Begriff *„Persönlichkeitsprofile“* im VE-DSG ist sehr sinnvoll, da dieser immer zu grossen Unsicherheiten geführt hat und er überdies auch im ausländischen Recht kein bekannter Begriff ist. Neu soll *„Profiling“* verwendet werden. Profiling ist *„jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität“.* Ein Profiling ist nur mit der ausdrücklichen Einwilligung der betroffenen Person zulässig. Wer diese Einwilligung nicht einholt, begeht eine widerrechtliche Persönlichkeitsverletzung (vgl. Art. 23 Abs. 2 Bst. d VE-DSG). Gemäss dem Erläuternden Bericht ist massgebend, dass Daten im Hinblick auf die Untersuchung zentraler Persönlichkeitsmerkmale ausgewertet werden. Die Auswertung der Daten kann automatisiert oder nicht-automatisiert erfolgen.

Die Definition des Begriffs *„Profiling“* geht zu weit und auch weiter als die EU-DSGVO. Zukünftig wird beispielsweise jede schriftliche Qualifikation eines Mitarbeiters – ohne explizite Einwilligung des Betroffenen – als Persönlichkeitsverletzung betrachtet. Diese neue Bestimmung ist sehr heikel und nach unserem Dafürhalten ein unnötiges *„Swiss Finish“.* Profiling ist auf die automatisierte Bewertung von Personendaten zu beschränken. Ausserdem sind die Bedingungen zu reduzieren und anstatt einer Einwilligung lediglich eine Informationspflicht festzulegen.

Wir beantragen die Einschränkung des Profiling auf *„besonders schützenswerte Personendaten“* und auf die automatisierte Datenauswertung.

3.4. Auftragsbearbeiter (Art. 3 Bst. i VE-DSG)

Die Bestimmung von Art. 3 Bst. i VE-DSG ist zu ungenau und kann zu Missverständnissen führen.

Wir beantragen daher folgende Präzisierung des Wortlautes: *"… im Rahmen eines Rechtsgeschäfts mit dem Verantwortlichen Personendaten bearbeitet, wobei das Vorliegen eines Arbeitsverhältnisses nicht als Rechtsgeschäft im Sinne dieser Regelung gilt".*

4. Auftragsdatenbearbeitung (Art. 7 VE-DSG)

Die Zustimmungspflicht im (neuen) Art. 7 Abs. 3 VE-DSG zum Sub-Outsourcing ist fragwürdig. Interessanterweise muss in der Systematik der *„Verantwortliche“* die betroffene Person in der Regel nicht um Zustimmung bitten, wenn er ihre Daten outsourct. Der Outsourcer muss dann aber den Verantwortlichen um Zustimmung bitten, wenn er sub-outsourct.

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

Die Grundidee ist gut, es besteht allerdings das Risiko, dass sie in der Ausführung zu einer Verschärfung des DSG selbst führt. Es fehlen Kontrollmöglichkeiten und Rechtsschutzmechanismen. Auch aus Gründen der Gewaltentrennung sollte die Erstellung der Empfehlungen nicht durch den EDÖB selbst, sondern zwingend durch ein Fachgremium erfolgen. Nur durch den entsprechenden Praxisbezug können sachgerechte Lösungen erarbeitet werden. In der DSGVO wird die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Wir beantragen somit, dass die Empfehlungen der guten Praxis durch ein breit abgestütztes Fachgremium, in welchem neben anderen auch die Wirtschaft vertreten wird, erlassen werden, wobei der EDÖB über eine beratende Stimme verfügt.

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

Im geltenden DSG ist Art. 12 VE-DSG ein Teilanspruch des Auskunftsrechts. Positiv zu vermerken ist, dass der VE-DSG eine Vorreiterrolle beim *„Persönlichkeitsschutz“* von verstorbenen Personen einnimmt. Art.12 VE-DSG regelt die datenschutzrechtlichen Gegebenheiten nach dem Tod einer Person. Interessanterweise berücksichtigt dies jedoch die EU-DSGVO nicht, obwohl es hierzu seit Jahren

strittige Fälle gibt, z.B. die datenschutzrechtlichen Einstellungen von Facebook, wenn es um die Rechte der Angehörigen nach dem Tode eines Facebook Users geht. Gemäss dieser Regelung sind nebst den (gesetzlichen und eingesetzten) Erben weitere Personen auskunftsberechtigt.

Das Auskunftsrecht geht über den Auskunftsanspruch der Erben hinaus, was unseres Erachtens zu weit geht.

Wir beantragen somit, dass das Auskunftsrecht entsprechend der erbrechtlichen Regelungen auf Erben beschränkt wird.

7. Informationspflicht bei der Beschaffung von Personendaten (Art. 13 VE-DSG)

Nach Art. 13 Abs. 1 VE-DSG muss der Verantwortliche die betroffene Person über die Beschaffung von Personendaten informieren. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. Diese Bestimmung soll gemäss dem Erläuternden Bericht vom 21. Dezember 2016 die Transparenz bei der Datenbearbeitung verbessern, was eines der zentralen Ziele der Revision ist.

Der Wortlaut der Bestimmung ist zu unklar und der Begriff *„Beschaffen"* wird nicht definiert, auch nicht in Art. 3 VE-DSG. Im Übrigen geht diese Bestimmung über die EU-DSGVO hinaus. Uns stellt sich insbesondere die Frage, ob ein Internet Research und die Verwertung der darin gefundenen Information zu einer Person bereits unter diese Bestimmung fällt und diese Person informiert werden müsste, was natürlich viel zu weit gehen würde. Die Bestimmung führt zu einer grossen Unsicherheit bei den Unternehmen, auch deshalb weil ein Verstoss sanktioniert wird (vgl. Art. 50 Abs. 1, Bst. a und b, Ziff. 1 und 2 VE-DSG).

Im geltenden DSG besteht die Informationspflicht nur bei der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Als wesentliche Änderung im VE-DSG soll diese Pflicht nun bei allen Daten gelten. Durch eine solche umfassende Informationspflicht würde nicht mehr Transparenz geschaffen, sondern es würde einfach zu einem Mehr an Information kommen, was letztlich der Transparenz zuwiderlaufen würde (kontraproduktive Informationsüberflutung). Eine standardisierte Information in Form von AGB oder in einer generellen Datenschutzerklärung muss genügen. Alles andere ginge viel zu weit.

Wir beantragen daher, dass der Wortlaut nochmals einer kritischen Betrachtung zu unterziehen sei und die Informationspflicht beschränkt wird auf „besonders schützenswerte Personendaten und Persönlichkeitsprofile".

8. Informations- und Anhörungspflichten bei einer automatisierten Einzelentscheidung (Art. 15 VE-DSG)

Der Bundesrat erachtet die Einführung des neuen Begriffs *„automatisierte Einzelentscheidung"* für notwendig, weil diese Entscheidungen in allen Wirtschaftsbereichen immer häufiger und teilweise auf der Grundlage falscher Daten getroffen werden. Eine automatisierte Einzelentscheidung besteht, wenn ohne menschliches Dazutun eine Auswertung von Daten erfolgt, die zu einer konkreten Entscheidung gegenüber der betroffenen Person führt (siehe Erläuternder Bericht zum Vorentwurf).

Dieses Thema ist eine Blackbox, da der Umfang der Informationspflicht unklar ist. Die Übernahme ist aufgrund des E-SEV 108 erforderlich, es wäre allerdings empfehlenswert, den Begriff der *"automatisierten Einzelentscheidung"* in Artikel 3 zu erläutern/definieren. Der völlig uneingeschränkte Äusserungsanspruch geht zudem sehr weit und kann insbesondere auch in kleinen und bescheidenen Verhältnissen zu einem unverhältnismässig und sachlich nicht gerechtfertigten hohen administrativen Aufwand führen. Die Informations- resp. Anhörungspflicht ist eine Einmischung in den zivilrechtlichen Willensbildungsvorgang einer Person bzw. eines Unternehmens. Ein Richtigkeitsgebot würde auch genügen. Auch mit einer allgemeinen Information könnte hier die notwendige Transparenz betreffend die automatisierte Einzelentscheidung erreicht werden, um das effektiv bestehende Bedürfnis nach dem Schutz gegen negative Entscheidfindung mittels falscher Daten zu befriedigen, ohne jedoch die Entwicklung der digitalen Wirtschaft und Gesellschaft übermässig zu behindern.

Wir beantragen, dass der Begriff *„automatisierte Einzelentscheidung“* in Art. 3 VE-DSG zu erläutern ist.

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

Die Datenschutz-Folgenabschätzung ist eine neue Pflicht im VE-DSG, womit die Anforderungen von Art. 8^{bis} Abs. 2 E-SEV 108 sowie die Artikel 27f. der Richtlinie (EU) 2016/680 verwirklicht werden sollen. In der Verordnung (EU) 2016/679 ist eine ähnliche Vorschrift enthalten. Die Datenschutz-Folgenabschätzung soll ein Instrument sein zur Erkennung und Bewertung von Risiken, die den betroffenen Personen durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Ein Verstoss gegen diese Norm wird sanktioniert (vgl. Art. 50 Abs. 1 Bst. c und Art. 51 Abs. 1 Bst. d VE-DSG).

Die gesetzliche Umschreibung ist ausserordentlich vage *("voraussichtlich", "erhöht", "Risiko"*) und kann infolgedessen angesichts der aus einer Missachtung dieser Regelung resultierenden Folgen seitens der Daten verarbeitenden Person zu erheblichen Unsicherheiten führen. Auch der Erläuternde Bericht vom 21. Dezember 2016 legt sich nicht fest, was das *„erhöhte Risiko“* ist. In Verbindung mit der Regelung in Artikel 17 VE-DSG (Meldung von Verletzungen des Datenschutzes) führt diese Bestimmung zu einer drastischen Verschiebung der Schwelle zu einem inkriminierten Verhalten insbesondere auch zu Ungunsten kleinerer und mittlerer Betriebe bzw. bei einfachen Verhältnissen, wo wohl oft auch *"unbewusste"* Datenverarbeitungen in Unkenntnis der gesetzlichen Regelungen erfolgen (z.B. Onlineshop für Bastelartikel mit ausschliesslich Schweizer Kundschaft). Hier wird sehr oft ein die Strafbarkeit rechtfertigendes Unrechtsbewusstsein fehlen.

Die Regelung in Art. 16 Abs. 3 VE-DSG (Benachrichtigung des EDÖB über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen) geht zu weit. Es würde eine Konsultation bei erheblichen Restrisiken genügen. Die geplante Strafbarkeit für private Personen (Busse bis CHF 500‘000.-), wenn die Meldung unterlassen wird, ist nicht angemessen (vgl. Art. 51 Abs. 1 Bst. d VE-DSG).

Die Dreimonatsfrist für Einwände in Art. 16 Abs. 4 VE-DSG ist viel zu lang.

Wir beantragen, dass der Wortlaut von Art. 16 VE-DSG präzisiert und die unbestimmten Begriffe definiert werden sollen sowie die Reduktion der Frist für Einwände auf ein angemessenes Mass zu reduzieren ist.

10. Meldung von Verletzungen des Datenschutzes (Art. 17 VE-DSG)

Art. 17 VE-DSG ist eine neue Bestimmung. Sie verwirklicht (siehe Erläuternder Bericht zum Vorentwurf) die Anforderungen von Art. 7 Abs. 2 E-SEV 108 sowie von Artikel 30 der Richtlinien (EU) 2016/680. In Artikel 33 der Verordnung (EU) 2016/679 ist eine ähnliche Regelung enthalten. Jede Art der unbefugten Bearbeitung, auch die unbefugte Löschung, gilt als Verletzung des Datenschutzes. Die Meldung hat ab Kenntnisnahme unverzüglich zu erfolgen. Ein Verstoss gegen diese Meldepflicht wird sanktioniert (vgl. Art. 50 Abs. 2 Bst. d VE-DSG).

Die Übernahme einer solchen Bestimmung ist aufgrund von übergeordnetem Recht (E-SEV 108) erforderlich. Unternehmen werden somit entsprechende Verfahren schaffen müssen. Hier besteht aber der Fehlgedanke, dass der Datenschutz massgeblich verbessert wird, wenn die Unternehmen bei festgestellter Datenschutzverletzung eine staatliche Institution informieren müssen. Wichtig ist, dass man die Ausnahmebestimmung weit auslegt, also rasch annehmen darf, dass kein *„Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person“* besteht.

Gemäss dem Wortlaut von Art. 17 Abs. 1 VE-DSG hat der Verantwortliche die Meldung *„unverzüglich“* zu machen. Damit enthält die Bestimmung einen unbestimmten Begriff, der zu Verunsicherung führt. Damit besteht auch die Gefahr eines vorschnellen Handelns durch den Verantwortlichen. Nach Abs. 2 von Art. 17 muss der Verantwortliche die betroffene Person informieren, wenn es deren Schutz erfordert oder der EDÖB dies verlangt. Aufgrund der Systematik und dem Wortlaut muss damit zuerst die Meldung an den EDÖB gemacht und erst anschliessend der Betroffene informiert werden. Für die Unternehmen hat diese Meldepflicht einen sehr hohen administrativen und finanziellen Aufwand zur Folge. Für den Verantwortlichen, der diese Meldung machen muss, kommt diese einer zwingenden Selbstanzeige gleich. Unter Umständen muss er sich damit selbst belasten, was nicht angehen kann.

Wir beantragen die Herstellung der Äquivalenz zum EU-Recht. Konkret soll die Meldepflicht auf die Verletzung des Schutzes personenbezogener Daten eingegrenzt werden.

11. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 18 VE-DSG)

Diese neue Regelung soll die Anforderungen von Artikel 8 Ziff. 3 E-SEV 108 sowie von Artikel 20 Abs. 1 der Richtlinie (EU) 2016/680 verwirklichen. Auch in Artikel 25 der Verordnung (EU) 2016/679 ist eine ähnliche Bestimmung enthalten. In Abs. 1 geht es primär darum, Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten, dass sie insbesondere den Grundsätzen nach Artikel 4 VE-DSG entsprechen. So kann beispielsweise dafür gesorgt werden, dass Daten in regelmässigen Abständen gelöscht oder standardmässig anonymisiert werden (siehe Erläuternder Bericht zum Vorentwurf). Abs. 2 führt neu die Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen (*Privacy by Default*) ein.

Zwar sind *Privacy by Default* und *Privacy by Design* stets gehörte Begriffe. Aber auch hier sind wir der Auffassung, dass diese für das CH-Recht nicht wirklich eine Neuerung bedeuten. Die geltenden Bearbeitungsgrundsätze sehen bereits entsprechende Pflichten vor. Hier haben wir nun aber eine Normierung, was den Fokus auf die Einhaltung erhöhen, weiteren Aufwand generieren und damit im Ergebnis zu einer massiv geringeren Datenverfügbarkeit führen wird. Dadurch würden die wirtschaftlichen Nutzungsmöglichkeiten stark eingeschränkt.

12. Weitere Pflichten (Art. 19 VE-DSG)

Wir regen an, zu Art. 19 Bst. b VE-DSG an geeigneter Stelle festzuhalten, dass an den Nachweis zum *„unverhältnismässigen Aufwand"* keine hohen Anforderungen gestellt werden.

13. Auskunftsrecht (Art. 20 VE-DSG)

Das Auskunftsrecht ergänzt die Informationspflicht des Verantwortlichen und bildet die zentrale Grundlage dafür, dass die betroffene Person ihre Rechte nach diesem Gesetz überhaupt wahrnehmen kann. Das Auskunftsrecht ist ein subjektives höchstpersönliches Recht. Ein Verstoss gegen diese Pflicht wird sanktioniert (vgl. Art. 50 Abs. 1 Bst. a VE-DSG).

Das alte Auskunftsrecht war bereits umfassend genug.

Falls doch an einer Änderung festgehalten werden soll, sollten diese Informationen nur auf Antrag der betroffenen Person mitgeteilt werden müssen. Zudem sollte in Absatz 3 das Wort *„Zustandekommen"* gestrichen werden, da dieser Vorgang in der Regel ein schützenswertes Geschäftsgeheimnis darstellt und für den Empfänger auch nicht sehr aufschlussreich sein dürfte.

Wir beantragen, den Umfang des geltenden Auskunftsrechts auch im VE-DSG beizubehalten.

14. Wegfall von Artikel 28 DSG (Beratung Privater) wäre ein Verlust

Falls diese Bestimmung vollständig wegfällt, ist es ein Verlust. Es bestand die Möglichkeit, informelle und pragmatische Auskünfte zu erhalten. Die im Erläuternden Bericht zum Vorentwurf zu Art. 43 Abs. 1 VE-DSG erwähnte Beratungsmöglichkeit muss daher unbedingt aufrechterhalten werden.

Es sei daher Art. 28 DSG auch im VE-DSG beizubehalten.

15. Sanktionen bei Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 50 VE-DSG)

Bei den in Art. 50 ff. VE-DSG vorgesehenen Sanktionen handelt es sich um strafrechtliche Sanktionen, die sich direkt gegen die verantwortlichen natürlichen Personen richten. Der maximale Betrag der Busse, der heute gemäss Artikel 106 Abs. 1 StGB bei 10 000 Franken liegt, soll auf 500 000 Franken erhöht werden. Dies ist eine deutliche Verschärfung gegenüber der geltenden Regelung.

Gemäss unserer Beurteilung sanktioniert diese vorgeschlagene neue Regelung teilweise reine *"Ordnungsvorschriften"* mit teilweise völlig unverhältnismässig hohen Bussen, welche in keiner Relation zum möglichen Unrechtsgehalt der Daten verarbeitenden Person stehen.

Dem EDÖB soll keine Kompetenz eingeräumt werden, Verwaltungssanktionen zu sprechen. Um die Rechtmässigkeit und die Akzeptanz solcher Verfügungen sowie die Wahrung der Verfahrensrechte sicherzustellen, hätte die Organisation des EDÖB verändert werden müssen, beispielsweise analog zur Schweizerischen Wettbewerbskommission. Darauf wurde insbesondere mit Blick auf die Kosten verzichtet. Der Bundesrat erachtet es als vorteilhafter, Zuwiderhandlungen im Rahmen eines Strafverfahrens zu ahnden, welches die Garantien des Strafprozessrechts bietet (siehe Erläuternder Bericht vom 21. Dezember 2016). Auch die Empfehlungen EDÖB sollen (nach wie vor) keinen bindenden Charakter haben. Im Vergleich zum europäischen Ausland sind die Befugnisse des EDÖB somit nach wie vor sehr eingeschränkt, was dem Ansinnen, seine Funktion im Zuge der Revision des DSG zu stärken, entgegenspricht.

Zudem fehlt dem neuen Sanktionsregime eine klare Umschreibung der einschlägigen Tatbestände. Dies dürfte zu grosser Unsicherheit und letztendlich dazu führen, dass seitens der Verantwortlichen (i) aus Angst vor einer Sanktionierung mehr unternommen wird als notwendig (Overengineering), und dadurch (ii) die Informationsflut gegenüber den betroffenen Personen unverhältnismässig umfangreich wird, was dem Ziel der erhöhten Transparenz wohl eher zuwider laufen dürfte.

Es soll ausserdem eine starke *„Pönalisierung“* allfälliger (bewusster oder *„unbewusster“*, leichter oder grober) Verstösse gegen die gesetzlichen Regelungen erfolgen. Der Kreis der neuen (Straf-)Tatbestände wie auch die Höhe der mit diesen verbundenen Strafen ist in vielen Teilen unangemessen und unverhältnismässig sowie nicht zielführend. Bei der Festlegung des *„Pflichtenkatalogs“* der Daten verarbeitenden Person wird nicht bzw. unzureichend berücksichtigt, zu welchen Zwecken und in welchem örtlichen Rahmen Daten verarbeitet werden. Somit hat die Betreiberin eines kleinen *„Onlineshops“*, welche sich ausschliesslich an Kunden in der Schweiz richtet bzw. ihre Produkte ausschliesslich in der Schweiz absetzt, die gleichen (sehr umfassenden und mit Strafe sanktionierten) Regelungen zu beachten und einzuhalten wie ein grösseres Unternehmen, welches mit ihrer Tätigkeit erhebliche Umsätze erzielt oder grenzüberschreitend Handel betreibt. Die Aufwendungen zur Sicherstellung der Einhaltung der (datenschutz)rechtlichen Regelungen können jedoch aus finanziellen und personellen Mitteln bei kleineren und mittleren Unternehmen nicht in gleicher Weise geleistet werden wie in grösseren bzw. grossen Unternehmen.

Es wäre somit wünschenswert, wenn bei der Umschreibung des Pflichtenkatalogs (wie allenfalls auch der Sanktionen bei Pflichtwidrigkeiten) der Daten verarbeitenden Personen noch vermehrt der Situation kleinerer und mittlerer Betriebe Rechnung getragen würde. Wir erachten es bei eingeschränktem örtlichem Tätigkeitsbereich insbesondere auch nicht für zwingend notwendig, die sehr strengen Vorgaben des EU-Rechts *„tel quel“* zu übernehmen.

In Art. 50 Bst. e VE-DSG wird ein neues Unterlassungsdelikt vorgeschlagen. Es ist nicht klar, welche Personen wegen eines Verstosses gegen dieses Unterlassungsdelikt bestraft werden können sollten. Offen ist, welche Personen eine *"allgemeine Garantenstellung"* für die Pflicht zur Meldung von Verletzungen des DSG trifft. Diese Bestimmung, welche keinerlei sachliche und persönliche Einschränkungen enthält, setzt Unternehmen dem Risiko erpresserischer Handlungen bzw. Drohungen aus.

Sie dürfte letztlich auch geeignet sein, das Denunziantentum zu fördern, was schliesslich dem Ziel eines wirksamen und effizienten Datenschutzes wohl gar auch diametral entgegenlaufen wird. Auch die strafrechtliche Sanktionierung einer Missachtung einer Verfügung des EDÖB ist in der Schweizerischen Rechtsordnung grundsätzlich untypisch und schiesst über das Ziel hinaus.

Die Bestimmungen von Art. 50ff. VE-DSG sind nochmals einer kritischen Betrachtung zu unterziehen und maximal die Äquivalenz zum EU-Recht herzustellen.

16. Einwilligung von Kindern nicht geregelt

Ein weiterer, wichtiger Punkt stellt u.E. die **nicht geregelte Einwilligung von Kindern** dar.

In der DSGVO wurde das Mindestalter für die Abgabe einer rechtswirksamen Einwilligung in die Verarbeitung von personenbezogenen Daten von ursprünglich 13 Jahre auf 16 Jahre angehoben.
Die Einwilligung von Kindern ist zwar im Schweizer ZGB grundsätzlich geregelt, sollte jedoch auch im Schweizerischen Datenschutzgesetz geregelt sein.

Wir beantragen, die Einwilligung von Kindern im VE-DSG zu regeln.

Abschliessend möchten wir uns nochmals für die Möglichkeit bedanken, uns zur Revision des Datenschutzgesetzes vernehmen zu lassen.

Für Rückfragen oder ergänzende Auskünfte in diesem Zusammenhang stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

EXPERTsuisse

Dr. Lukas Imark
Präsident der Kommission für Rechtsfragen

lic. iur. Sergio Ceresola
Mitglied der Geschäftsleitung
Regulatorisches & Support