Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

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

31. März 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin

Im Dezember 2016 haben Sie uns eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung:

Kernanliegen der Wirtschaft

Der Umgang mit Daten ist für die Digitale Wirtschaft zentral. «Entfaltungsmöglichkeit der Unternehmen» und «Vertrauen der Nutzer» beschreiben die Leitlinien einer optimalen Datenpolitik. In diesem Sinne gilt es, die übergeordneten Ziele der Strategie «Digitale Schweiz» des Bundesrates im Fokus zu behalten: Zu berücksichtigen ist dabei insbesondere auch der Nutzen der Daten für den digitalen Fortschritt und für die Ausschöpfung des wirtschaftlichen Potentials im Interesse der Konsumenten und Unternehmen. Eine einseitige Orientierung lediglich an potentiellen Risiken ist verfehlt. Zentral ist deshalb: Innovation und Entwicklung dürfen durch den Datenschutz nicht behindert werden.

Die Regulierung hat sich am Verhältnismässigkeitsprinzip zu orientieren und alle Eingriffe sind auf das Minimum zu beschränken. Entsprechend ist im Datenschutzgesetz für die Unternehmen ein Maximum an Flexibilität zu wahren. Spielräume im Verhältnis zum internationalen Recht sowie das etablierte System der Selbstregulierung sind so weit als möglich zu nutzen. Die diversen im Vergleich zum EU-Raum überschiessenden Regelungen sind anzupassen. Dabei soll die Totalrevision insbesondere

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

auch genutzt werden, um bestehende Bestimmungen im Hinblick auf ihre Praxistauglichkeit zu hinterfragen und an die technologische Entwicklung anzupassen.

Die Kernanliegen der Wirtschaft lassen sich in folgende Themenbereiche unterteilen: Profiling, Selbstregulierung, Informations- und Meldepflichten sowie Aufsicht und Sanktionen. Hieraus ergeben sich die folgenden Hauptforderungen:

— Der Begriff «**Profiling**» ist auf automatisierte Bewertungen von Personendaten einzuschränken und die Bedingungen dazu sind stark zu reduzieren (Information statt Einwilligung);

— Die Initiative für Empfehlungen der guten Praxis muss stets zwingend von (Branchen)Verbänden ausgehen. Die **Selbstregulierung** ermöglicht es mittels Bezug zur Praxis, sachgerechte Lösungen zu entwickeln. Der betriebliche Datenschutzbeauftragte ist auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen;

— Diverse **Informations- und Meldepflichten** sind überschiessend. Sie bedeuten unverhältnismässigen Aufwand und generieren eine regelrechte «Flut» an Informationen und Meldungen. Abzulehnen sind auch die damit verbundene Offenlegung von Geschäftsgeheimnissen und die Pflicht, sich selbst zu belasten. Gesamthaft wirken sich die vorgeschlagenen Pflichten innovations- und wettbewerbshindernd aus. Sie sind dem vom Vorentwurf angestrebten risikobasierten Ansatz entsprechend substantiell zu reduzieren. Dies betrifft insbesondere automatisierte Einzelfallentscheide, Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzverstössen. Darüber hinaus braucht es eine Relativierung der Kostenlosigkeit des Auskunftsrechts und weitere, griffige Massnahmen, um dem Missbrauch des Datenschutzrechtes zu datenschutzfremden Zwecken entgegenzuwirken;

— Ein weiterer umfassender Kritikpunkt ist das vorgeschlagene **Sanktionssystem**: Private, strafrechtliche Sanktionen sind weder verhältnismässig noch zielführend. Es ist ein tragbares, mit den rechtsstaatlichen Grundsätzen vereinbares Sanktionssystem zu implementieren. Gleichzeitig ist eine zu grosse Machtfülle des EDÖB zu verhindern. Die Wirtschaft skizziert ein eigenes Sanktionsmodell als Grundlage für die Entwicklung eines alternativen Lösungsansatzes.

1. Einleitende Bemerkungen

Ein angemessenes und wirksames Datenschutzgesetz ist für die Wirtschaft von grosser Bedeutung. Dieses muss Raum für die wirtschaftliche Entwicklung lassen sowie der Rechts- und Investitionssicherheit dienen. Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und der Nutzung des damit verbundenen wirtschaftlichen Potentials. Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich demgegenüber innovationshemmend aus. Sie können der Wettbewerbsfähigkeit von Unternehmen auf nationaler Stufe, vor allem aber auch im internationalen Umfeld schaden. Zu weitgehende Bestimmungen, welche den Individuen ihre Handlungsfähigkeit absprechen, führen zudem zu einer Bevormundung der Bürgerinnen und Bürger.

Angesichts der dynamischen technologischen aber auch der internationalen Entwicklungen im Bereich Datenschutz ist für die Schweiz von Bedeutung, dass sie mit modernen Regelungen den Austausch international und insbesondere mit dem EU-Raum nicht unnötig einschränkt. Damit die Schweizer Regulierung aus Sicht der EU ein «angemessenes Schutzniveau» i.S.v. Art. 45 DSGVO gewährleistet, reicht es jedoch, wenn sie die grundlegenden Garantien einhält (vgl. Erw. 104 DSGVO / US-EU Privacy Shields). Die entsprechenden Kriterien sind in der EU-Verordnung abschliessend aufgezählt. Daneben hat sich das Schweizer Datenschutzrecht auch an der Konvention 108 des Europarates zu orientieren, welche für die Schweiz verbindlich gilt, dies unter Berücksichtigung auch der Richtlinie (EU) 2016/680.

Hierbei ist innerhalb der internationalen Vorgaben ein Maximum an Flexibilität für den Schweizer Standort zu sichern; die Wirtschaft darf nicht durch übertriebene Bestimmungen («Swiss Finish») mit unnötigem administrativen und finanziellen Aufwand belastet werden. Dieser wäre gerade auch aus einer gesamtheitlichen Sicht kontraproduktiv, weil solche Schweizer Besonderheiten einen einheitlichen internationalen Datenraum verhindern und damit auch zulasten der Schweizer Unternehmen wettbewerbsverzerrend wirken würden. Nur die Verwendung von Begriffen, welche mit den internationalen Texten übereinstimmen, erleichtert den internationalen Verkehr.

Auf Basis des Vorentwurfes unter Berücksichtigung der Rückmeldungen der Mitglieder und der Arbeiten in der Arbeitsgruppe Datenschutz sowie in der Rechtkommission wurde der Anpassungsbedarf aus einer gesamtwirtschaftlichen Sicht erarbeitet. Im Folgenden wird aufgezeigt, wie die Regelungen bzw. deren Reichweite mit Sicht auf ihre Praxistauglichkeit abgestimmt werden müssen und wo grundsätzlichere Anpassungen vorzunehmen sind.

2. Zweck

Die Zweckbestimmung ist anzupassen. Gerade auch unter Berücksichtigung der Strategie des Bundesrates für eine «digitale Schweiz» ist der Zweck um «die Förderung des freien Verkehrs der Personendaten» zu ergänzen. Dies entspricht dem Ziel des erläuternden Berichts, dass durch die Datenschutzgesetzrevision «die Wettbewerbsfähigkeit der Schweiz gewährleistet und verbessert werden [soll], namentlich indem die Bekanntgabe von Daten ins Ausland erleichtert wird. Eine entsprechende Zielsetzung kennt auch die europäische Verordnung.

3. Geltungsbereich

Berücksichtigung bereichsspezifischer Datenschutzbestimmungen
Einige Mitglieder haben darauf hingewiesen, dass in verschiedenen Bereichen (z.B. in der Humanforschung) spezielle Bestimmungen zu datenschutzrechtlichen Fragen bestehen. Diese sind teilweise auf Verordnungsebene festgeschrieben. Es ist für die betroffenen Unternehmen zentral, dass sie sich weiterhin auf die entsprechenden Regelungen verlassen können. Es sollte festgehalten werden, dass Spezialbestimmungen im Datenschutzrecht den Regelungen des DSG vorgehen bzw. dass der Grundsatz «lex specialis » umfassend zu verstehen ist.

Kein Schutz für juristische Personen
Die Abschaffung des Datenschutzes für Unternehmen analog der DSGVO und E-SEV 108 wird begrüsst. Dieser hat in der Praxis kaum eine Rolle gespielt. Zudem wird der Persönlichkeitsschutz von ZGB 28 und der Schutz von Geschäftsgeheimnissen dadurch nicht tangiert. Einzelunternehmen und Mitglieder von Personengesellschaften, die im Handelsregister eingetragen sind, sind jedoch weiterhin vom Schutz des DSG umfasst. Es wurde angeregt, dass hier dieselbe Regelung zum Geltungsbereich wie für juristische Personen gelten sollte.

Neues Missbrauchspotential beim Auskunftsrecht
Der VE-DSG sieht neu vor, dass das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren zur Anwendung gelangen soll. Dieser erweiterte Geltungsbereich birgt erhebliches Missbrauchspotential beim Auskunftsrecht (Beweisbeschaffung über die zivilprozessualen Editionsrechte hinaus). Es braucht griffige Mechanismen, welche dem Rechtsmissbrauch oder der nicht vorgesehenen Anwendung dieser Bestimmung im Zivilprozess oder im Strafverfahren entgegenstehen (vgl. nachfolgend Ziff. 11).

Regelung des räumlichen Anwendungsbereichs / IPR
Im VE-DSG fehlt eine Regelung zum räumlichen Anwendungsbereich des Gesetzes. Von wirtschaftlicher Seite her besteht der Wunsch, den räumlichen Anwendungsbereich nicht übermässig auszudehnen und damit den Status quo beizubehalten. Dies bedarf einer gleichzeitigen Anpassung der entsprechenden Regelung im IPRG, damit der Geltungsbereich des Schweizerischen Datenschutzgesetzes in räumlicher Hinsicht relativiert werden kann.

4. Begriffe

Definition der Personendaten
Art. 3 lit. a VE-DSG sieht keine Definition der Bestimmbarkeit vor. Es ist zu konkretisieren was unter «bestimmbaren Personendaten» zu verstehen ist. Zudem ist wie im geltenden Recht klarzustellen, dass mit dem Begriff «Daten» stets *Personen*daten gemeint sind.

Einschränkung der Definition der besonders schützenswerten Personendaten
Die Ausweitung des Begriffs der «besonders schützenswerten Personendaten» auf die entsprechenden Definitionen der genetischen und biometrischen 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 der Konvention 108. Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Einschränkung der Definition des Profiling
Die Definition des Begriffs «Profiling» ist im VE-DSG sehr breit gefasst und geht deutlich über die entsprechende Regelung der EU hinaus. In der DSGVO hängt die Zulässigkeit des Profiling von der Wahrnehmung der betroffenen Interessen ab. Nur in Fällen, in denen das Profiling Teil einer *automatischen Entscheidung* wird und rechtliche Wirkung erzeugt, gelten andere Vorschriften. Der VE-DSG vermischt die beiden Institute: Erfasst ist auch das «menschliche», d.h. manuelle Profiling (z.B. eine schriftliche Mitarbeiterbeurteilung oder die Alterskapitalberechnung einer Versicherung) sowie nicht-personenbezogene Daten. Dies stellt eine unzulässige Ausweitung des Geltungsbereiches dar und steht damit im Widerspruch zu Art. 2 Abs. 1 VE-DSG.

Die Definition des Begriffes ist analog der DSGVO auf die *automatisierte* Auswertung von *Personen*daten zu begrenzen. Zudem ist die Auswertung, bzw. Analyse keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte auswirkt. Die Bestimmung sollte daher anstatt «Auswertung» analog der DSGVO den Begriff «Bewertung» verwenden.

Einführung des betrieblichen Datenschutzbeauftragten
Es besteht klar der Wunsch, auf freiwilliger Basis eine Regelung zur Bezeichnung eines betrieblichen Datenschutzbeauftragten vorzusehen. Dies soll im Gegenzug mit einer entsprechenden Erleichterung bei den Pflichten unter dem DSG verknüpft werden (vgl. nachfolgend, Ziff. 8.2). In diesem Sinne ist auch eine Definition des betrieblichen Datenschutzbeauftragten erforderlich.

5. Grundsätze

Klare Terminologien
Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zweckes unnötigerweise mit dem Zusatz der «klaren» Erkennbarkeit. Diese Anpassung an die Terminologie des DSGVO ist in diesem Falle verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert damit auch Rechtsunsicherheit. Der Zusatz ist nicht erforderlich und zu streichen.

Dies gilt auch für den Begriff der «eindeutigen» Einwilligung von Art. 4 Abs. 6 VE-DSG: Damit wird lediglich wiederholt, was bereits heute unter dem risikobasierten Ansatz gilt. Der Zusatz ist ebenfalls wegzulassen. Auch wann eine Einwilligung «ausdrücklich» sein soll, ist nicht klar. Jedenfalls muss auch passives Verhalten als gültige Einwilligung gelten, damit weiterhin die im Massengeschäft unumgänglichen Allgemeinen Geschäftsbedingungen (AGB) verwendet werden können. Das Erfordernis der Einwilligung für das Profiling muss gänzlich gestrichen werden (vgl. Ziff. 13).

Keine Nachführungspflicht
Die permanente Nachführungspflicht geht zu weit und ist nicht praktikabel. Der 1. Satz von Art. 4 Abs. 5 VE-DSG ist entsprechend ersatzlos zu streichen.

6. Auslandtransfer

Unnötige Wiederholung von Grundsätzen
Art. 5 Abs. 1 VE-DSG wiederholt bereits statuierte Grundsätze und ist im Kontext von Art. 5 verwirrend und überflüssig. Der Absatz ist deshalb zu streichen.

Keine zwingende Feststellung durch den Bundesrat
Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung würde i.d.R. besser durch den Verantwortlichen, gestützt auf eigene Abklärungen und Kenntnisse, erfolgen. Es erscheint zudem problematisch, wenn sich der Verantwortliche nur auf die Einschätzung des Bundesrates verlässt, selbst, wenn ihm eine schwerwiegende Gefährdung von Persönlichkeitsrechten bekannt ist. Die Bestimmung ist dahingehend anzupassen, dass die Feststellung des Bundesrates keine abschliessende ist und diese nur subsidiär zum Zuge kommt.

6.1 Informations- und Genehmigungspflicht

Unklare und widersprüchliche Kategorisierung der Garantien
Die Unterscheidung in Art. 5 Abs. 3 VE-DSG zwischen «spezifischen» und «standardisierten» Garantien ist unklar und macht aus Sicht der Praxis keinen Sinn. Erschwerend kommt hinzu, dass die standardisierten Garantien einer Genehmigung durch den EDÖB bedürfen.

Auch Binding Corporate Rules (BCR) unterliegen der Genehmigungspflicht, diese stellen aber eine Untergruppe der spezifischen Garantien dar. Für diese wiederum ist jedoch nur eine Informationspflicht vorgeschrieben. Dies ist widersprüchlich. Es sollte lediglich zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden und die Pflichten entsprechend angepasst werden.

Berücksichtigung von Geheimhaltungsinteressen
Spezifische Garantien sind in der Regel in Verträgen enthalten. Es ist praxisfern und insbesondere im Zusammenhang mit dem BGÖ problematisch, wenn diese alle dem EDÖB vorgelegt werden müssen.

Kürzung der Genehmigungsfrist
Für eine Genehmigung ist die vorgesehene Frist des EDÖB von 6 Monaten nicht praktikabel. Im Tagesgeschäft sind entsprechende Bewilligungen kurzfristig erforderlich. Mit derart ausgedehnten Fristen ist eine Verwendung solcher Garantien / BCR kaum noch möglich, da ein Unternehmen nach Vertragsabschluss nicht derart lange warten kann. Die Frist ist auf das heutige Mass von 30 Tagen zu kürzen und von einer unbeschränkt möglichen Verlängerung abzusehen. Der Beauftragte muss also innerhalb dieser Frist reagieren, ansonsten gelten die vorgelegten Garantien / BCR als genehmigt.

Zu berücksichtigen ist ferner, dass in gewissen Branchen auch 30 Tage viel zu lang sein können, da aufgrund der Umstände umgehend reagiert werden muss. Für die entsprechenden Sachverhalte liegen bereits heute Spezialregelungen vor, die der Genehmigungspflicht von Art. 5 VE-DSG weiterhin vorgehen müssen (z.B. von der FINMA, um Finanzinstituten die Einhaltung von Pflichten nach ausländischen Bestimmungen zu ermöglichen).

Alternativ: Keine Genehmigung durch den Beauftragten
Einzelne Mitglieder wünschen, die Genehmigung von standardisierten Garantien oder verbindlichen unternehmensinternen Datenschutzvorschriften (BCR) durch den Beauftragten ganz wegzulassen. Die Genehmigungspflicht würde zu einem erheblichen Mehraufwand für die Unternehmen und gegebenenfalls zu Projektverzögerungen führen. Gleichzeitig trage diese kaum etwas zum besseren Datenschutz bei, da das Unternehmen weiterhin selber in der Verantwortung stehe. Ein grenzüberschreitender Datenfluss würde durch diese Regelung erheblich erschwert. Lediglich die DSGVO (nicht die Konvention 108) sieht eine entsprechende Vorgabe vor. Es wird hier klar Raum für einen sich im Verhältnis zur DSGVO differenzierenden Regelungsansatz gesehen. Für ein «angemessenes Schutzniveau» ist die Genehmigung jedenfalls nicht nötig.

Keine Informationspflicht bei Vorliegen standardisierter Garantien
Die pauschale Informationspflicht von Art. 5 Abs. 6 VE-DSG im Zusammenhang mit standardisierten Garantien bringt keinen Mehrwert. Es geht hier um bereits genehmigte oder anerkannte Garantien. Dies ist nicht einmal in der DSGVO vorgesehen[1]. Die Bestimmung ist entsprechend zu streichen.

6.2 Ausnahmen

Keine Einwilligung «im Einzelfall»
Die in Art. 6 Abs. 1 lit. a VE-DSG vorgesehene Ausnahme der «Einwilligung im Einzelfall» ist weder sinnvoll noch notwendig. Nach den allgemeinen Grundregeln reicht für wiederkehrende Sachverhalte bei gleichbleibender Erkennbarkeit und Erwartung eine einmalige Einwilligung. Der Zusatz «im Einzelfall» ist zu streichen. Dies gilt auch für die «Bekanntgabe im Einzelfall» (Art. 6 Abs. 1 lit. d VE-DSG).

Erweiterung der Ausnahme i. Zh. mit Verträgen
Die Ausnahmebestimmung von Art. 6 Abs. 1 lit. b VE-DSG ist mit der DSGVO abzustimmen. Die Ausnahme ist auf diejenigen Fälle auszuweiten, in denen die betroffene Person nicht Vertragspartei ist, der betroffene Vertrag aber in ihrem Interesse ist oder zu ihren Gunsten abgeschlossen wurde.

Streichung Begriffe «Gericht» und «Verwaltungsbehörde»
Die Begriffe «Gericht» und «Verwaltungsbehörde» bei Art. 6 Abs. 1 lit. c VE-DSG sind zu streichen. Die Unterscheidung ist nicht erforderlich und es stellen sich schwierige Abgrenzungsfragen. Massgebend ist, dass die Datenbearbeitung zur «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen» erfolgt.

Keine Informationspflicht bei Vorliegen eines Ausnahmetatbestandes
Die in Art. 6 Abs. 2 vorgesehene Informationspflicht, dies trotz Vorliegen eines Ausnahmetatbestandes, ist unverhältnismässig und zu streichen. Eine entsprechende Bestimmung ist in der Konvention nicht vorgesehen. Nebst zu erwartender hoher Anzahl an Meldungen wäre auch die Information des EDÖB über heikle Verfahren und (Geschäfts-)geheimnisse problematisch (BGÖ).

7. Auftragsdatenbearbeitung

Keine Vergewisserungspflicht
Die in Art. 7 neu vorgesehene Vergewisserungspflicht führt zu massivem Mehraufwand beim Outsourcing der Datenbearbeitung. Es ist unklar, welche Pflichten dem Auftragsdatenbearbeiter überbunden werden sollen. Die Vergewisserungspflicht widerspricht dem prinzipienbasierten Ansatz des VE-DSG und die Präzisierung ist gerade in Bezug auf projektspezifische Herausforderungen kontraproduktiv. Die Bestimmung ist zu streichen. Dies gilt auch für den letzten Satz von Absatz 3 bezüglich Präzisierung weiterer Pflichten des Auftragsbearbeiters durch den Bundesrat.

Reduzierte Anforderungen an die Einwilligung
Die Anforderung einer «schriftlichen» Zustimmung ist vor dem Hintergrund der heutigen Geschäftsprozesse, dies insbesondere auch aufgrund der komplexen Dienstleistungsverhältnisse, nicht praxistauglich. Eine dokumentierte Zustimmung reicht aus; Schriftlichkeit i.S.v. Art. 13 OR ist nicht erforderlich. Es

[1] Vgl. dazu EuGH-Entscheid Schrems und Entscheid der EU-Kommission vom 16.12.2016 (keine erneute Einwilligung im Einzelfall).

ist eine technologieneutrale Präzisierung vorzunehmen, dass, dies auch im Einklang mit der Bestimmung in der EU, eine generelle Einwilligung für den Beizug von Sub-Auftragsdatenbearbeitenden und eine Information im konkreten Fall ausreicht.

8. Selbstregulierung

8.1 Empfehlungen der guten Praxis

Begrüssenswerte Selbstregulierung aber keine Empfehlungen des Beauftragten
Grundsätzlich sind Empfehlungen der guten Praxis in Anlehnung an das bestehende und bewährte Konzept der Selbstregulierung der Branchen zu begrüssen. Der wesentliche Vorteil liegt darin, dass so sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präsentiert werden können. Dazu müssen themenspezifische Wünsche der Branche tatsächlich in die Regelung einfliessen. Die im VE-DSG vorgesehene Kompetenz des EDÖB, Empfehlungen der guten Praxis auf eigene Faust auszuarbeiten, widerspricht aber dem Zweck des Instituts. Es fehlen Kontrollen und Rechtsschutzmechanismen. Entsprechend besteht die Gefahr, dass der EDÖB «falsche» oder unverhältnismässige Empfehlungen im Alleingang, ohne institutionelle Kontrolle, verabschiedet. Aufgrund der Fiktion der Rechtmässigkeit von Art. 9 Abs. 1 VE-DSG würde er damit faktisch zum Gesetzgeber. Dem stünde noch verschärfend entgegen, dass eigene Empfehlungen der interessierten Kreise nur mittels Genehmigung durch den EDÖB festgelegt werden könnten. Unter der DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Daraus ergibt sich, dass die Bestimmung der VE-DSG dahingehend anzupassen ist, dass die Initiative für Empfehlungen der guten Praxis stets zwingend von (Branchen)Verbänden ausgehen muss. Dies würde der Tradition der Selbstregulierung entsprechen und brächte den Vorteil mit sich, dass solche Richtlinien von Experten mit starkem Bezug zur Praxis verfasst werden. Dies würde es ermöglichen, sachgerechte Lösungen zu entwickeln, bei denen der Beauftragte durch die Genehmigung immer noch das letzte Wort hat. Die genehmigten Empfehlungen der guten Praxis sind vom EDÖB zu publizieren.

Vermutung der Richtigkeit statt Fiktion / Geltung auch für Auftragsdatenbearbeiter
Die Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung der Datenschutzvorschriften schliesst, ist ausserdem nicht zielführend. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig / unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.

8.2 Betrieblicher Datenschutzbeauftragter

Einführung auf freiwilliger Basis gekoppelt mit Freistellung von Meldepflichten
Der VE-DSG verlangt richtigerweise nicht die breite Einführung eines betrieblichen Datenschutzbeauftragten. Das Institut eines betrieblichen Datenschutzbeauftragten sollte aber weiterhin vorgesehen werden. Dies als Option für die Unternehmen kombiniert mit der Freistellung von allfälligen Meldepflichten gegenüber dem EDÖB (z.B. bei der Datenschutz-Folgenabschätzung). Ein betrieblicher Datenschutzbeauftragter könnte als zentrale Stelle die Pflichten für die Unternehmen oder ganze Unternehmensgruppen wahrnehmen. Damit liessen sich Doppelspurigkeiten vermeiden. Auch würde dadurch eine Anlaufstelle für Auskunftsbegehren geschaffen. Dies würde eine Flexibilisierung und gerade für grössere Unternehmen Erleichterungen mit sich bringen, ohne dass KMU belastet würden. Letztlich würde auch die Zugänglichkeit des Datenschutzes für die betroffene Person verbessert.

Die betrieblichen Datenschutzbeauftragen sind auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen (z.B. bei Art. 15, 16 und 17 VE-DSG). Die entsprechende Person darf jedoch im Rahmen von Sanktionen nicht übermässig exponiert werden (siehe hierzu unten, Ziff. 14.3).

9. Daten einer verstorbenen Person

Keine Regelung im DSG

Art. 12 VE-DSG erscheint im VE-DSG als Fremdkörper. Die Regelung könnte zu Rechtsunsicherheiten führen. Der Nachweis der persönlichen Beziehungen im Zusammenhang mit dem schutzwürdigen Interesse ist in der Praxis kaum zu erbringen. Für Geschäftsdaten bestehen gemäss spezialgesetzlichen Regelungen weitreichende legitime Dokumentations- und Archivierungspflichten, weshalb die pauschale Formulierung des Löschungsrechts nicht zielführend ist. Erben sind bereits durch die erbrechtliche Universalsukzession ausreichend legitimiert, geeignete, interessenwahrende Massnahmen vorzukehren. Die Bestimmung ist deshalb im VE-DSG zu streichen. Eine Regelung wäre an geeigneter Stelle (z.B. im ZGB) vorzusehen, dies aber zu einem späteren Zeitpunkt im Rahmen einer umfassenden Regelung in Bezug auf die Verfügung über Daten und nicht ausschliesslich aus einer datenschutzrechtlichen Sicht.

10. Pflichten

Keine pauschale Anwendung

Die pauschale Anwendung der vorgesehenen Pflichten auf alle Geschäftsmodelle und Branchen ist nicht sachgerecht und wäre mit enormem Aufwand verbunden. Es gilt, ein gestuftes Modell vorzusehen: Strengere Bestimmungen wären dabei für Geschäftsmodelle vorzusehen, welche besonders sensible Datenbearbeitungen umfassen, wie dies typischerweise bei spezifischen Marketing-Dienstleistern und Data-Minern der Fall ist. Auch bei den Pflichten ist ein risikobasierter Ansatz vorzukehren. Zudem können branchenspezifische Regelungen weitergehende Pflichten vorsehen.

Erleichterungen für Unternehmensgruppen

Gleich strenge Regelungen für die interne Weitergabe von Daten in Konzernverhältnissen sind nicht verhältnismässig. Analog Art. 47 DSGVO ist eine Bestimmung zu internen Datenschutzvorschriften für die erleichterte gruppeninterne Datenweitergabe in das DSG aufzunehmen. Dabei ist auch der Einsatz eines allfälligen internen Datenschutzbeauftragten (vgl. oben) zu berücksichtigen.

10.1 Informationspflichten

Risikobasierte Transparenzpflicht als Leitlinie

Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen aufgrund des öffentlich-rechtlichen Charakters der Bestimmungen und den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Die vorgesehene massive Ausdehnung der Informationsmenge führt zu einer Überinformation der betroffenen Personen und würde sich damit kontraproduktiv auf die Transparenz auswirken. Die Regel muss grundsätzlich im Sinne einer risikobasierten Transparenzpflicht überarbeitet werden. Es sollte zudem explizit die Möglichkeit von standardisierten Informationen (z.B. mittels AGB oder Erklärungen auf Websites) eingeführt werden. Dies auch deshalb, weil oft nicht klar ist, worüber genau informiert werden muss.

Konkret ist die Informationspflicht auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektiven) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person zu beschränken. Ausserdem ist klarzustellen, dass sich die Information (und damit auch die Richtigkeit und Vollständigkeit der Daten) auf den Zeitpunkt der Datenbeschaffung bezieht und nicht auf nachträgliche Änderungen. Dies schliesst auch eine Pflicht zur Nachinformation klar aus. Als Kontaktdaten des Verantwortlichen muss eine klare und definierte Funktionsbeschreibung ausreichen, da die natürliche Person innerhalb einer Funktion wechseln kann.

Präzise und einheitliche Terminologien

Unklar ist die Differenzierung zwischen «Beschaffung» und «Bearbeitung» und die in Abs. 3 verwendeten Begriffe «Dritte» sowie «Empfängerinnen und Empfänger». Es sollten präzisere und einheitliche Terminologien verwendet werden. Es ist auch fraglich, warum der Vorentwurf den Begriff «Beschaffung» statt wie in der DSGVO vorgesehen «Erhebung» verwendet. Dadurch können sich (nachteilige) Abweichungen im Informationszeitpunkt ergeben.

Keine Mitteilung von Identität und Kontaktdaten der Auftragsdatenbearbeiter

Die Pflicht zur Mitteilung der Identität und der Kontaktdaten sämtlicher Auftragsdatenbearbeiter ist gegenüber dem EU-Recht klar überschiessend. Sie ist weder sinnvoll noch erforderlich. Die Offenlegung der oft für untergeordnete Tätigkeiten mandatierten Auftragsdatenbearbeiter ist nur mit unverhältnismässigem Aufwand zu bewerkstelligen und greift zudem in berechtigte eigene Datenschutzinteressen sowie Geschäftsgeheimnisse der Unternehmen ein. Schliesslich ist unklar, wann genau über was informiert werden muss. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist bereits Gegenstand von Art. 7 VE-DSG. Diese Zusatzanforderung ist zu streichen.

Keine Mitteilung bei indirekter Datenbeschaffung

Die vorgesehene Informationspflicht bei der indirekten Datenbeschaffung geht zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein. Das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus sind solche direkten Informationspflichten nicht erforderlich; eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist zu streichen.

Erweiterung und Präzisierung der Ausnahmen

Die Ausnahmebestimmung von Art. 14 Abs. 3 lit. a VE-DSG ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur selten aus einem Gesetz. Häufiger sieht ein Gesetz zwingende Abklärungspflichten vor, welche mit Geheimhaltungspflichten verbunden sind und welche damit mit einer Einschränkung der Informationspflicht einhergehen. Die Bestimmung ist zu präzisieren und mit typischen Beispielen zu ergänzen (z.B. Abklärungen im Zusammenhang mit Geldwäscherei, Terrorismusbekämpfung und Korruption). Ausserdem können sich Verpflichtungen auch aus einem Vertrag ergeben. Eine weitere Ausnahme ergibt sich bei Datenbearbeitungen, die für eine Rechtsdurchsetzung erforderlich sind. Auch dies ist zu ergänzen.

Für die Einschränkung der Berufung auf überwiegende private Interessen, d.h. auf Fälle, in denen die Personendaten nicht Dritten bekannt gegeben werden, gibt es keine sachlichen Gründe. Besonders bei Konzernverhältnissen würde daraus ein enormer administrativer Mehraufwand resultieren. Sollte die betroffene Person durch die Bekanntgabe beeinträchtigt sein, so wäre dies im Rahmen der allgemeinen Interessensabwägung von Art. 24 VE-DSG zu berücksichtigen. Die Einschränkung ist damit zu streichen.

Die Bestimmung von Art. 14 Abs. 5 VE-DSG ist nicht praktikabel und zu streichen; diese würde dazu führen, dass ständig einzelne Interessensabwägungen überprüft werden müssten. In grossen, komplexen Organisationen ist dies nicht zu bewerkstelligen.

10.2 Automatisierte Einzelfallentscheide

Begrenzung des Anwendungsbereichs und der Pflichten; insb. keine Anhörungspflicht
Die Reichweite der neu eingeführten Informations- und Anhörungspflicht sowie Auskunftsrechte bei automatisierten Einzelfallentscheiden ist zu weitgehend. Zwar kennen die Konvention 108 und die EU eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE-DSG ist jedoch viel breiter: Der VE-DSG unterscheidet stärker zwischen Profiling und automatisieren Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen, welche so wohl nicht beabsichtigt waren: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden. Die Automatisierung ist ein zentraler Punkt der Digitalisierung und im heutigen wirtschaftlichen Umfeld von grundsätzlicher Bedeutung. Davon profitieren auch die Kunden, z.B. durch Objektivität der Entscheidung, schnellere Prozesse und damit besserer Nutzererfahrung sowie einer attraktiven Preisgestaltung.

Insbesondere das vorgesehene Äusserungsrecht der betroffenen Person bringt keinen Mehrwert; es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Die Offenlegung, wie bestimmte Entscheide zustande gekommen sind, betrifft zudem oft auch Geschäftsgeheimnisse.

Die Bestimmung ist entsprechend auf schwere Fälle, bzw. solche, die erhebliche Auswirkungen auf die Rechtstellung der betroffenen Person haben, zu begrenzen. Der Wortlaut ist an die entsprechende Bestimmung in der DSGVO anzupassen (insbesondere «Beeinträchtigung» statt «Wirkung» und «erhebliche» in Bezug auf beide Alternativen). Auch dann sind sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen sind. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung i.S.d. Gesetzessystematik ist ausreichend. Das Äusserungsrecht und der damit zusammenhängende Art. 20 Abs. 3 (Auskunftsrecht) sind zu streichen. Dies ist aufgrund des Derogationsrechts der Mitgliedstaaten der EU für die Äquivalenz nicht abträglich (vgl. Art. 22 Abs. 2 lit. c DSGVO).

10.3 Datenschutz-Folgenabschätzung

Beschränkung und Präzisierung / keine Pflicht des Auftragsdatenbearbeiters
Das in Art. 16 neu eingeführte Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) ist zu weit gefasst. Die offene und dadurch unklare Formulierung führt dazu, dass für praktisch alle Datenbearbeitungen vorgängig aufwändige Abklärungen durchgeführt werden müssten. Besonders problematisch ist die vorgesehene Sanktionierung bei Verstoss. Analog der DSGVO ist eine Konkretisierung sowie Beschränkung auf Fälle vorzunehmen, bei denen ein *«hohes Risiko*» besteht bzw. ein solches nach vorgenommenen Massnahmen zur Risikominimierung *verbleibt*. Darüber hinaus ist zu präzisieren, dass ein Risiko für eine Persönlichkeitsverletzung bestehen muss. Der Begriff «oder die Grundrechte» ist sodann zu streichen: Das Schweizer Recht kennt, anders als das europäische Recht, keine direkte Drittwirkung der Grundrechte. Schliesslich ist der Auftragsdatenbearbeiter von der Pflicht

auszunehmen. Dieser verfügt regelmässig nicht über die notwendigen Angaben, sondern unterliegt den Entscheidungen des Verantwortlichen.

Meldung nur bei *Rest*risiko und Verkürzung der Frist / Streichung der Meldepflicht
Die anschliessenden umfangreichen Meldepflichten sind ein klares «Swiss Finish»; sie sind unverhältnismässig und greifen in die Geheimsphäre der Unternehmen ein. Die zu erwartende «Meldeflut» ist für eine angemessene Reaktion des EDÖB kontraproduktiv. Problematisch ist auch die lange Frist, innert welcher der EDÖB Einwände mitteilen oder später eine Untersuchung einleiten kann. Damit werden falsche Anreize gesetzt. In der Gesamtheit bringt die Bestimmung keinen Mehrwert, führt jedoch zu erheblichen Rechtsunsicherheiten und innovationshemmenden Verzögerungen. Die Forderung der Konvention 108, bei geplanten Datenbearbeitungen Risiken einzuschätzen, wurde bereits durch Art. 11 VE-DSG (Datensicherheit) erfüllt. Schliesslich bestehen weitere Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen (z.B. im Bankengesetz). Doppelte Überwachungen sind aus Effizienzgründen zu vermeiden.

Eine Meldung an den EDÖB sollte nur dann erfolgen müssen, wenn *nach* ergriffenen Schutzmassnahmen ein grosses *Rest*risiko verbleibt. Es ist klar zu regeln, welche Informationen weitergeleitet werden müssen und wie damit bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz umgegangen wird. Weiter ist die vorgesehene Reaktionszeit des EDÖB von drei Monaten, welche zudem laufend verlängert werden kann, auf einen Monat zu reduzieren.

Einige Mitglieder sprechen sich für die gänzliche Streichung der Meldepflicht und folglich auch von Art. 16 Abs. 4 VE-DESG aus. Eine Meldung solle erst erfolgen, wenn eine Verletzung des Datenschutzes passiert ist, nicht bereits aufgrund von Risiken. Auch die E-SEV 108 verlange nicht, die Behörden von der Datenschutz-Folgenabschätzung zu informieren. Eine Ausnahme der Meldepflicht sollte zumindest für Unternehmen mit einem betrieblichen Datenschutzbeauftragten vorgesehen werden.

10.4 Meldepflichten

Beschränkung auf Verstösse mit gravierenden Folgen
Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse (inkl. Datenverluste) an den EDÖB (Data Breach Notification) ist stark einzuschränken. Sie erfasst weit mehr Fälle als die DSGVO, welche diese Pflicht nur für Verletzungen von Sicherheitsmassnahmen vorsieht, die zusätzlich zu einem Bruch oder Verlust des Gewahrsams an den Daten führen. Zudem kann die vorgesehene Ausnahme sachlogisch nie angerufen werden, da eine «falsche» Datenbearbeitung per Definition immer eine Verletzung von Persönlichkeitsrechten ist.

Eine Pflicht ohne Eingrenzung in qualitativer und quantitativer Weise würde uferlos; jeder noch so geringe Verstoss müsste gemeldet werden, um den Sanktionsfolgen zu entgehen. Der Beauftragte sähe sich mit einer weiteren Meldungsflut konfrontiert und wäre ausser Stande, allfällig wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. Die Meldepflicht führt auch zu einem Konflikt mit dem strafrechtlichen Grundprinzip von «nemo tenetur»[2]. Schliesslich wäre eine «unverzügliche» Meldung auch in zeitlicher Hinsicht nicht umsetzbar, da zuerst hinreichende Informationen gesammelt werden müssen. Zudem besteht die Gefahr, durch vorschnelles Handeln Geschäfts- oder Berufsgeheimnisse zu verletzen. So sieht die DSGVO eine Frist von bis zu 72 Stunden vor.

[2] Vgl. mehr dazu unter „Aufsicht und Sanktionen“.

Der Begriff des «Data Breach» sollte analog E-SEV und DSGVO formuliert werden. Die Pflicht wäre damit auf Verstösse mit gravierenden Folgen zu beschränken, bei welchen ein Kontrollverlust an den Daten vorliegt. Als weiteres qualitatives Kriterium müsste die Tatsache ergänzt werden, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann. Dies z.B. mittels Unterstützung in Fällen, welche von den Verantwortlichen nicht mehr aus eigener Kraft bereinigt werden können. Weiter ist die Bestimmung durch ein quantitatives Element zu konkretisieren, z.B. auf Fälle, in welchen Daten von mindestens 100'000 Personen betroffen sind. Eine Meldung beim EDÖB muss den Schutz vor Sanktionen zur Folge haben (vgl. nachfolgend Ziff. 14.3).

10.5 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Anpassung der Reichweite und Überführung zu den Sicherheitsbestimmungen
Die Formulierung von Art. 18 VE-DSG geht ebenfalls über jene der DSGVO hinaus. Zudem gehört diese systematisch zu Art. 11 VE-DSG (Sicherheit von Personendaten). Diese Bestimmung deckt die Anforderungen von «privacy by design» bereits. Art. 18 VE-DSG ist zu streichen, resp. in Art. 11 zu integrieren. Die Reichweite ist an das EU-Recht anzupassen.

10.6 Weitere Pflichten

Verzeichnis statt allgemeine Dokumentationspflicht / Ausnahme für kleinere Unternehmen
Die allgemeine Dokumentationspflicht von Art. 19 lit. a VE-DSG ist bezüglich Inhalt und Umfang unklar und geht über die vergleichbare Bestimmung der EU hinaus. Die Pflicht ist analog der DSGVO auf die Pflicht zur Erstellung «eines Verzeichnisses für regelmässige Datenbearbeitungen» einzuschränken. Die Pflicht, Datenschutzverstösse zu dokumentieren, ist zu weitgehend. Darüber hinaus ist auch eine Ausnahme der Pflicht für kleinere Unternehmen (z.B. analog EU mit weniger als 250 Mitarbeitenden oder am Umsatz gemessen) vorzusehen, sofern sie in Bezug auf den Datenschutz keine risikoreiche Tätigkeit ausüben. Aus systematischen Gründen sollte auch diese Bestimmung in Art. 11 VE-DSG integriert werden.

Fokus auf Praxistauglichkeit bei der Informationspflicht an Dritte
Die Reichweite der neu vorgesehenen Pflicht, Dritten die Berichtigung, Löschung oder Vernichtung von Daten zu melden, geht sehr weit und ist in der Praxis nicht umsetzbar. Eine solche Meldepflicht ist von E-SEV 108 nicht und von der DSGVO nicht in dieser Form vorgesehen. Die DSGVO kennt eine entsprechende Meldepflicht nur unter gewissen Voraussetzungen im Zusammenhang mit dem «Recht auf Vergessen». Der VE-DSG erfasst demgegenüber auch unbedeutende Vorgänge; im täglichen Arbeitsprozess werden ständig Daten berichtigt, gelöscht oder vernichtet (z.B., weil ein Kunde bezahlt hat oder die Daten schlicht keine Relevanz mehr haben). Die Auswirkungen dieser Meldepflicht wurden offenbar unterschätzt. Zu deren Bewältigung müsste eine neue Infrastruktur aufgebaut werden, welche sämtliche Empfänger über Jahrzehnte hinweg verwaltet. Eine betroffene Person ist besser in der Lage zu beurteilen, welche Daten für welche Empfänger (noch) von Interesse sind. Gerade solche Informationsansprüche der betroffenen Person sind aber bereits unter Art. 25 VE-DSG vorgesehen. Die Informationspflicht an Dritte ist analog der DSGVO auf Fälle zu beschränken, in welchen die betroffene Person die Nachinformation aus berechtigten Gründen verlangt hat.

11. Auskunftsrecht

Massnahmen gegen missbräuchliche Auskunftsbegehren
Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und hängige Verfahren bringt grosse Aufwendungen mit sich. Umso mehr, weil ein Auskunftsbegehren im Datenschutzsystem der Schweiz nie unverhältnismässig sein kann, da auch untergeordnete Datenschutzinteressen für einen Anspruch ausreichen. Gerade auch die vorgesehene umfassende Kostenlosigkeit des Auskunftsrechts führt zu Fehlanreizen: Es sind keine Massnahmen vorgesehen, welche es den Unternehmen erlauben würden, dem Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken Einhalt zu gebieten (vgl. Ziff. 3).

Es sind griffige Massnahmen gegen den Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken vorzusehen: Die Kostenlosigkeit ist wie in Art. 2 VDSG zu relativieren, so z.B. bei unverhältnismässigem Aufwand und bei Ersuchen zu nicht ausschliesslich datenschutzrechtlichen Zwecken. Zudem sind weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. bei Art. 21 VE-DSG).

Verhinderung einer möglichen Informationsflut bei automatisierten Einzelfallentscheiden
Eine «Rechenschaftspflicht» in Bezug auf automatisierte Entscheide in der vorgesehenen detaillierten Form ist unverhältnismässig: Informationen darüber, wie bestimmte Entscheide zustande kommen, gehören zum Geschäftsgeheimnis. Durch die gewählte Formulierung wäre jedes Ergebnis, d.h. jeder Entscheid erfasst. Dies würde zu einem zusätzlichen Administrativaufwand führen, ohne dass damit mehr Transparenz geschaffen würde. Im Gegenteil: Kunden würden Informationen erhalten, mit denen sie gar nichts anzufangen wissen (z.B. warum sie eine Werbeanzeige nicht erhalten haben).

Die geforderte Information über Vorliegen einer automatisierten Einzelfallentscheidung (Art. 20 Abs. 2 lit. e VE-DSG) sollte in allgemeiner Weise erfolgen. Die Bestimmung von Art. 20 Abs. 3 VE-DSG sollte in Art. 15 VE-DSG integriert werden. Dessen Grundsätze («erhebliche Auswirkung») wären dabei einzuhalten. Es muss klargestellt werden, dass das Auskunftsrecht nur von der jeweils tatsächlich betroffenen Person ausgeübt werden kann. Zudem ist ein Verweis auf die Einschränkungen des Auskunftsrechts bzw. der Informationspflichten (Art. 21 i.V.m. 14 VE-DSG) anzubringen.

12. Ausnahmetatbestände

Ausweitung der Ausnahmen
Die vorgesehenen Ausnahmetatbestände gemäss Art. 14 VE-DSG sind zu eng formuliert und nicht konsistent. Die Informationspflicht sollte immer entfallen, wenn die Information nicht möglich oder unzumutbar ist. Eine Beschränkung auf Fälle der indirekten Beschaffung oder in denen keine Weitergabe an Dritte erfolgte ist nicht nachvollziehbar. Die Bestimmung ist entsprechend anzupassen.

Es sind Ausnahmen, auch in Hinblick auf die rechtsmissbräuchliche Geltendmachung des Auskunftsrechts, für folgende bearbeiteten Daten vorzusehen:

- Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen;

- Aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption;

— Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden;

— Rein intern bearbeitete Daten;

— Daten über Drittpersonen;

— Unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.

Übergabe der Informationen an Dritte bei Missbrauchsverdacht
Um Missbräuche zu verhindern, ist zudem vorzusehen, dass bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben werden können. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen. Eine Möglichkeit bestünde darin, dass der EDÖB den Entscheid über Herausgabe in Form einer anfechtbaren Verfügung vorlegt (vgl. analoge Regelung in Art. 8 Abs. 2 BPI).

13. Besondere Bestimmungen für die Datenbearbeitung durch private Personen

Keine ausdrückliche Einwilligung beim Profiling
Gemäss Art. 23 Abs. 2 lit. d VE-DSG gälte Profiling automatisch als Persönlichkeitsverletzung, wenn nicht vorgängig eine ausdrückliche Einwilligung eingeholt wird. Diese gesetzliche Vermutung stellt einen unbegründeten partiellen Paradigmenwechsel im Schweizer Datenschutzrecht dar (von grundsätzlicher Erlaubnis der Datenbearbeitung unter Einhaltung bestimmter Voraussetzungen zum Verbot mit Erlaubnisvorbehalt). Das Erfordernis der ausdrücklichen Einwilligung beim Profiling ist entsprechend zu streichen. Durch eine entsprechende Information kann genug Transparenz geschaffen werden. Eine Regelung hat unter Art. 15 VE-DSG zu erfolgen.

Klare und erweiterte Rechtfertigungsgründe
Der Ausdruck «möglicherweise» in Art. 24 Abs. 2 VE-DSG schafft Rechtsunsicherheit. Die aktuelle Bestimmung (Art. 13 Abs. 2 DSG) wurde unnötigerweise geändert und sollte beibehalten werden.

Art. 24 Abs. 2 lit. a VE-DSG sollte analog Art. 6 Abs. 1 lit. b VE-DSG Verträge berücksichtigen, die zu Gunsten oder im Interesse der betroffenen Person geschlossen werden.

14. Aufsicht und Sanktionen

Das vorgeschlagene Sanktionsmodell wurde in unserer internen Vernehmlassung breit kritisiert. Angesichts dieser Kritik und der Bedeutung der Thematik für die Schweizer Wirtschaft wird zum Thema Aufsicht und Sanktionen in detaillierterer Form Stellung genommen. Zudem präsentieren wir im Folgenden eine Grobskizze für einen alternativen Vorschlag für ein im Datenschutzgesetz zu integrierendes Sanktionsmodell.

Verschiedene Fachspezialisten aus der Wirtschaft sind gerne bereit, den Lösungsansatz zusammen mit weiteren interessierten Kreisen, beispielsweise im Rahmen einer vom Bundesamt für Justiz angelegten Arbeitsgruppe, zu vertiefen und eine ausgearbeitete Lösung zu entwickeln.

14.1 Ausgangslage

Anders als der VE-DSG setzen die Konvention 108 und die EU-Verordnung in erster Linie auf Verwaltungssanktionen gegen Unternehmen. Bei der Regelung der Sanktionierung von Datenschutzverletzungen besteht gemäss den europäischen Bestimmungen ein erheblicher Spielraum: Die Konvention verlangt im Wesentlichen *geeignete gerichtliche und nicht-gerichtliche Sanktionen und Rechtsmittel* (Art. 10 E-SEV 108). Die DSGVO (und auch die Richtlinie) sprechen von *wirksamen, verhältnismässigen und abschreckenden Sanktionen.* Es ist dabei den Mitgliedsstaaten überlassen zu entscheiden, ob Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind (Erw. 149 und 152).

14.2 Kritik am Vorentwurf und weitere Überlegungen

Die Wirtschaft ist bei der Abwägung verschiedener Sanktionsmodelle zum Schluss gekommen, dass die im VE-DSG vorgesehenen Sanktionen und insbesondere der Weg über das Strafrecht nicht zielführend sind:

<u>Persönliche Strafbarkeit der Mitarbeitenden</u>
Die Mitarbeitenden eines Unternehmens geraten durch die persönliche Strafbarkeit zu stark in den Fokus der Sanktionen. Verschärft wird dies durch die Höhe der Bussen und die vorgesehene Möglichkeit, sogar fahrlässiges Handeln zu bestrafen. Damit wird der risikobasierte Ansatz, der mit der Revision verfolgt wird, untergraben.

Strafrechtliche Sanktionen führen dazu, dass Mitarbeitende in Zukunft selbständig jeden (möglichen) Verstoss bei den Behörden melden müssen. Dies birgt das Risiko, dass sie sich gegenseitig anzeigen, um nicht selbst ins Visier der Strafbehörde zu geraten. Der VE-DSG bietet zudem Dritten viele Anknüpfungspunkte (sobald eine Datenerhebung stattgefunden hat), um Anzeige zu erstatten. Dies kann zum Unterlaufen der intern definierten Datenschutz-Governance und zu Unruhen innerhalb der Unternehmen führen sowie entsprechende Reputationsschäden nach sich ziehen. Entsprechende Meldungen bergen ausserdem die Gefahr, selbst wiederum zu Verletzungen des Datenschutzes zu führen.

Verurteilte Mitarbeitende wären sowohl intern als auch extern stark exponiert. Es dürfte daher mittelfristig schwierig werden, qualifiziertes Personal zu finden, das bereit ist, die Verantwortung mit den einhergehenden Risiken zu tragen. Die Folge wäre ein sukzessives Abfallen der Qualität im Bereich der Datenbearbeitung.

Die persönliche Strafbarkeit der Mitarbeitenden entspricht auch nicht der von anderen Schweizer Gesetzen vorgesehen Linie (vgl. KG, UWG, FMG, BEHG), bei welchen der Fokus klar auf der Sanktionierung der Unternehmen liegt.

Die strafrechtliche Sanktionierung würde schliesslich insbesondere die KMU stark belasten. Bei übersichtlichen Verhältnissen ist die Identifikation fehlbarer Mitarbeitenden relativ einfach; entsprechend bestünde ein Anreiz für die Strafverfolgungsbehörden, gerade bei solchen Unternehmen unverhältnismässig streng vorzugehen.

<u>Verstoss gegen strafrechtliche Grundprinzipien</u>
Problematisch sind die im VE-DSG vorgesehenen Mitwirkungspflichten angesichts des im Strafrecht vorherrschenden Grundsatzes des «nemo tenetur» bzw. des Selbstbelastungsverbotes. Die Pflicht, Datenschutzverstösse zu melden, käme faktisch einer Pflicht zur Selbstanzeige gleich. Der VE-DSG geht von einer verschuldensunabhängigen Sanktionierung aus und steht damit im Widerspruch zum

Verschuldensprinzip: Bei Vorliegen des objektiven Tatbestandes wird direkt darauf geschlossen, dass auch der subjektive Tatbestand erfüllt ist. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind offen formuliert (vgl. Art. 16 Abs. 1 VE-DSG: *"…vorgesehene Datenbearbeitung [führt] voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person*"). Dies ist mit dem strafrechtlichen Bestimmtheitsgebot bzw. einer hinreichenden Voraussehbarkeit einer Strafbarkeit nicht vereinbar.

Umfang von potentiellen Verstössen und Meldungen
Datenbearbeitungen stellen innerhalb der Unternehmen eine alltägliche Aktivität dar. Unternehmen können im Zeitalter der Digitalisierung nicht mehr wählen, ob eine entsprechende Handlung vorzunehmen ist oder nicht. Damit unterscheidet sich das Datenschutzrecht beispielsweise vom Kartellrecht. Im VE-DSG sind kaum Erheblichkeitsschwellen vorgesehen. Folglich würde jede geringfügige Unregelmässigkeit in alltäglichen Datenbearbeitungsvorgängen eine Datenschutzverletzung darstellen. Die daraus resultierende Mitteilungsmenge an den Beauftragten sowie die drastischen Sanktionsfolgen wären höchst problematisch.

Strafkatalog
Im Kern entspricht der Strafkatalog grundsätzlich den europäischen Bestimmungen. Hingegen werden die Berufspflichten erheblich verschärft und es wird sogar eine Freiheitsstrafe als Sanktion vorgesehen. Diese Ausweitung des Berufsgeheimnisses ist als überschiessende Bestimmung klar abzulehnen; es können in dieser Hinsicht nicht alle Berufe mit jenen von Art. 321 StGB gleichgesetzt werden.

Fazit
Die strafrechtlichen Sanktionen des VE-DSG, die gegen Mitarbeiter eines Unternehmens ausgesprochen werden können, sind weder verhältnismässig noch zielführend. Diese stehen im Widerspruch zu einer Vielzahl von schweizerischen strafprozessualen Prinzipen. Die auf Risikoausgleich ausgerichteten Möglichkeiten des VE-DSG werden damit ausgehöhlt und der Interessensausgleich wird unnötig eingeschränkt. Gesamthaft geht das vorgeschlagene strafrechtliche Sanktionsmodell damit deutlich über die im europäischen Raum vorgesehenen Sanktionen, die in erster Linie verwaltungsrechtlicher Natur sind, hinaus.

14.3 Vorschlag der Wirtschaft für ein mögliches Sanktionsmodell im DSG

Aufgrund der vorangehenden Überlegungen haben wir eine Grobskizze für ein alternatives Sanktionsmodell ausgearbeitet. Nicht strafrechtliche Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen sollen dabei im Vordergrund stehen.

Auch bei Verwaltungsstrafen ergeben sich verschiedene Problemfelder, gerade auch aus rechtsstaatlicher Sicht. Das nachfolgend skizzierte Modell berücksichtigt diese und schlägt ein auf die spezielle Konstellation des Datenschutzes angepasstes, verwaltungsrechtliches Sanktionsmodell vor. Dieses soll effizient ausgestaltet sein, die richtigen Anreize setzen und den Anforderungen an ein faires Verfahren entsprechen.

Die einzelnen Regeln dieses Verwaltungsverfahrens müssen den besonderen Verhältnissen bei Verletzungen des Datenschutzgesetzes entsprechend ausgestaltet werden und dürfen wegen den unterschiedlichen in Frage stehenden Rechtsgütern nicht einfach analog aus dem Kartellgesetz übernommen werden (insbesondere bezüglich der Sanktionen).

Grundsatz: verwaltungsrechtliche Sanktionen gegen Unternehmen

Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen. Anknüpfungspunkt sind dabei Organisationsmängel im Unternehmen. Lediglich subsidiär soll eine strafrechtliche Verfolgung von Mitarbeitenden möglich sein. Anzeigen sollen in der Regel durch die Unternehmen selbst erstattet werden. Im Ergebnis würde eine Anpassung des Sanktionsziels die Situation für die Datenbearbeitenden im Sinne einer Verbesserung des Datenschutzes im Unternehmen massgeblich entschärfen.

Eine Sanktionierung der Mitarbeitenden soll nur bei direkt vorsätzlichem Handeln, das sich gegen die Interessen des Unternehmens und/oder der betroffenen Person richtet, in Frage kommen. In diesem Zusammenhang ist eine Abstimmung mit den bereits im BT StGB vorgesehenen Strafbestimmungen erforderlich. Diese dürften für die Bestrafung der natürlichen Person meist schon ausreichen (z.B. Verletzung des Geschäftsgeheimnisses und unbefugte Datenbeschaffung). Der Kreis der potentiell strafrechtlich verantwortlichen Mitarbeitenden müsste zum Vornherein eingeschränkt werden (entsprechend Art. 29 StGB).

Angepasste Rolle des EDÖB und verbesserte Gewaltentrennung durch eine neu zu bildende Spruchbehörde

Eine Behörde, die gleichzeitig über Untersuchungs- und Spruchkompetenzen verfügt (wie bei Sanktionen mit verwaltungsrechtlichem Charakter üblich), hat die Tendenz, eine mit dem Prinzip der Gewaltenteilung nur schwer vereinbare Machtfülle zu erlangen. Die Verwaltungssanktionen sollten daher nicht von der Untersuchungsbehörde verhängt werden.

Die Ausstattung des EDÖB mit Spruchkompetenzen, sogar die im VE-DSG bereits vorgesehene Ausstattung mit Verfügungskompetenzen, kann dazu führen, dass zu viele Aufgaben bei EDÖB zusammenfliessen. Zusätzlich besteht die Gefahr, dass eine vertrauensvolle Zusammenarbeit mit den Unternehmen im Bereich der wichtigen Beratung beeinträchtigt wird. Ein auf Vertrauen basierender Austausch mit den Unternehmen ist für die Tätigkeit des Beauftragten jedoch von grundsätzlicher Bedeutung, dies umso mehr, als ihm gemäss VE-DSG die Aufgabe zukommt, Empfehlungen der guten Praxis zu erlassen.

Die Verfügungskompetenzen sowie die Sanktionskompetenz könnten entsprechend in einer neu zu bildenden «Datenschutz-Kommission» gebündelt werden. Diese könnte beispielsweise dem EDI oder EJPD angehängt sein. Ausschliesslich dieser kämen nebst der Sanktionskompetenz auch die Verfügungskompetenzen zu, dies gerade auch im Bereich vorsorglicher Massnahmen. Das Verhältnis zwischen «Datenschutz-Kommission» und EDÖB müsste präzisiert werden, insbesondere in Bezug auf die Überwachungs- und Untersuchungskompetenzen des Beauftragten i.S.v. Art. 40 f. VE-DSG. Als Alternative könnte auch der Weg über ein Gericht, z.B. am Sitz des EDÖB, geprüft werden (vgl. Verfahren in Kartellfragen in Deutschland).

In dieser Struktur würde der EDÖB seine bisherigen Aufgaben wahrnehmen und eine Vorselektion der ihm zugetragenen Fälle machen. Sollte sich in einem Fall eine mögliche Strafbarkeit abzeichnen, würde er die Angelegenheit der «Datenschutz-Kommission» weiterleiten. Bei Verfahren auf dieser zweiten Stufe würde die verwaltungsrechtliche Mitwirkungspflicht des Beauftragten wegfallen. Gegen Entscheide dieser Spruchbehörde stünde den Betroffenen der Weg zum Bundesverwaltungsgericht als Rechtsmittelinstanz offen.

Strafkatalog

Der Strafkatalog ist mit jenem der DSGVO abzugleichen, soll jedoch nicht darüber hinausgehen. Folgende Anpassungen sind erforderlich:

- Konkretisierung / Streichung der zu offen formulierten Tatbestände;

- Beschränkungen und Anpassungen bei den Pflichten der Verantwortlichen und Auftragsbearbeiter sind beim Strafkatalog zu berücksichtigen;

- Fokus auf wesentliche Bedrohung für die Privatsphäre der betroffenen Person;

- Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens in Bezug auf die betroffene Person orientiert. Zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung vorsätzlich vorgenommen wurde;

- Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten;

- Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab 2. Stufe des Verfahrens (siehe unten);

- Beschränkung der beruflichen Schweigepflicht auf Fälle, in denen die betroffene Person eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages).

Mitwirkungspflichten und Rechtfertigungs- und Strafmilderungsgründe

Neben der im Vorentwurf vorgesehenen Pflicht, Datenschutzverstösse bei den Behörden zu melden, besteht für die Unternehmen im verwaltungsrechtlichen Verfahren generell eine Mitwirkungspflicht. Wie oben kritisiert, läuft die Idee der anschliessenden Bestrafung im Rahmen eines Strafverfahrens diesem Konzept entgegen und verstösst zusätzlich gegen das Selbstbelastungsverbot. Ein kooperatives Verhalten, das letztlich einer raschen Schadensminderung dienen soll, muss gefördert werden. Unternehmen, die den Beauftragten über eine Verletzung der Datenschutzbestimmungen informieren, mit den Behörden kooperieren, Fehler aktiv korrigieren und grössere Risiken zu verhindern suchen, sollen mit einer Reduktion der Sanktion oder gar dem Absehen von einer Sanktion rechnen können (vgl. auch Art. 49a Abs. 2 KG). Dieser auf Schadensminderung ausgerichtete Ansatz entspricht den modernen Grundsätzen der Corporate Governance und fördert gleichzeitig das Ziel, ein hohes Datenschutzniveau zu erreichen. Gründe, die rechtfertigend oder zumindest strafmildernd wirken sollten, wären etwa:

- Compliance-Defense: Implementierung eines tauglichen Compliance-Programmes;

- Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Richtlinien, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden;

- Handeln nach Treu & Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (z.B. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art»;

- Wahrung berechtigter Interessen: Güterabwägung im Fall von Pflichtenkollision mit anderen zwingenden Rechtsregeln (z.B. unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse zur Abwendung eines Unternehmenskonkurses; vgl. Notstand, Art. 17 StGB);

- Rechts- und Sachverhaltsirrtum (vgl. Art. 13 und 21 StGB);

— Strafrechtliche Verfolgung eines Mitarbeitenden. Eine Anzeige gegen einen direktvorsätzlich handelnden Mitarbeitenden durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden;

— Aktive Schadensverminderung und Zusammenarbeit mit den Behörden.

Sanktionen

Datenbearbeitungen gehören zur täglichen Arbeit der Unternehmen. Datenschutzverletzungen können dementsprechend im Rahmen des Tagesgeschäftes geschehen. Dies muss bei der Festlegung der Sanktionshöhe einen Einfluss haben. Keinesfalls dürfen umsatzorientierte Ansätze zur Anwendung kommen. Dies wäre nicht sachgerecht, da Verletzungen des Datenschutzgesetzes kaum je in der Absicht erfolgen, den Umsatz oder Gewinn des Unternehmens zu erhöhen (anders als z.B. bei Kartellabsprachen). Deshalb ist eine maximale Obergrenze von CHF 500'000 für Bussen zu setzen. Zudem sind bei der Festlegung der Bussenhöhe die gesamten Umstände des Einzelfalles zu berücksichtigen, so z.B. die Schwere und die Auswirkungen des Verstosses sowie die oben genannten Rechtfertigungs- und Strafmilderungsgründe. Ebenso muss, in Anlehnung an die DSGVO, eine Konkurrenzklausel eingefügt werden: Bei gleichen oder miteinander verbundenen Datenbearbeitungsvorgängen, durch die vorsätzlich mehrere Bestimmungen des VE-DSG verletzt wurden, darf der Gesamtbetrag der Busse nicht denjenigen Betrag übersteigen, der für die schwerwiegendste Verletzung vorgesehen ist.

15. Übergangsfristen

Im VE-DSG fehlt eine umfassende Übergangsregelung. Die neuen und revidierten Bestimmungen werden die Prozesse der Unternehmen bedeutend beeinflussen. Es ist deshalb eine allgemeingültige Übergangsbestimmung von 2 Jahren aufzunehmen. Von einer Rückwirkung ist abzusehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Thomas Pletscher
Mitglied der Geschäftsleitung

Erich Herzog
Stv. Leiter Wettbewerb & Regulatorisches

Anhang: Skizze zum Sanktionsmodell