SUISSEDIGITAL

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

(vorab per Email in Word- und PDF-Fassung an: jonas.amstutz@bj.admin.ch)

Bern, 4. April 2017

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

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt SUISSEDIGITAL als Wirtschaftsverband der Schweizer Kommunikationsnetze gerne wahr.

SUISSEDIGITAL vertritt rund 200 privatwirtschaftlich und öffentlich-rechtlich organisierte Unternehmen aus der ganzen Schweiz von unterschiedlichster Grösse, welche aber mehrheitlich zum Kreis der KMU zu zählen sind. Diese versorgen mit ihren Kommunikationsnetzen und -dienstleistungen zahlreiche Geschäftskunden und über 2,5 Millionen Privathaushalte nicht nur in städtischen Gebieten, sondern auch in ländlichen Regionen. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir gestützt auf die zahlreich eingegangenen Inputs unserer Mitglieder wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

Verband für Kommunikationsnetze – Association des réseaux de communication
Kramgasse 5 – Postfach 515 – CH-3000 Bern 8 – T +41 31 328 27 28 – F +41 31 328 27 38 – info@suissedigital.ch – www.suissedigital.ch

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung" durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG

weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-Shop“ nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden.“). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands.“[2]

[1] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

[2] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen.“[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen“ Ergebnisse aufgrund der unzureichenden Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80‘000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365“ für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von

[3] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei.“[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40‘000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10‘000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5‘000 – 10‘000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5‘000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7‘500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5‘000 – 30‘000
Privacy by Default	1 – 40 Stunden		500 – 5‘000
Betriebliche Datenschutzbeauftragter		500 – 2‘000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5‘000

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

[6] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

[7] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

[8] In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14‘000 – 149‘000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1‘532‘160‘000, resp. im Durchschnitt von CHF 2‘520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen.“[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist

[9] 608‘000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

[10] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (<u>neu</u>)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*“ grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (<u>Beispiel</u>: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz“, Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis“ abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die <u>zum Zweck</u> der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten“. Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten“. Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten“ konsumiert. Der Begriff des „Profiling“ ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil“ des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling“ gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish“ versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage“ eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling“ verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist“ gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag“ (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag“ wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter“).
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten“ aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit“ einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig“, „freiwillig und eindeutig“, „ausdrücklich“ und die Abgrenzung zur blossen „Einwilligung“ (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig“, „eindeutig“ oder „ausdrücklich“ auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise“ völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen. [5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste. **Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen. **Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen“ Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche“ Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen“ reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish“ erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant“ zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves“ und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4.	
[3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten“ und „Persönlichkeitsprofilen“. Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat“. Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet; b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist; d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. **Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert. **Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. [3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle [1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. [2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen [1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. [2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. [3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1“ (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen. [2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen“. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen“ und ersetzen mit „seine Untersuchungen“. Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500‘000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1‘000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5‘000 – 30‘000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten“ wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom … *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom…. *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom ……	
Art. 114 Bst. f Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …….	
Art. 243 Abs. 2 Bst. d [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 … Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

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

Freundliche Grüsse

SUISSEDIGITAL – Verband für Kommunikationsnetze

Dr. Simon Osterwalder
Geschäftsführer / Rechtsanwalt

Stefan Flück
Leiter Rechtsdienst / Fürsprecher LL.M.