Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin
Karin Keller-Sutter
Bundeshaus West, 3003 Bern

Einreichung per Mail an: jonas.amstutz@bj.admin.ch

Bern, 13. Oktober 2021

Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Stellungnahme von digitalswitzerland

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zur «Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz» (VDSG) äussern zu können. Diese Gelegenheit nimmt der Verein digitalswitzerland gerne wahr.

1 Betroffenheit digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 240 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartnerin in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

2 Es braucht eine ausführliche Überarbeitung des Entwurfs

In einer zunehmend digitalisierten Wirtschaft ist es von zentraler Bedeutung, dass die Datenschutzgesetzgebung eine Balance zwischen dem angemessenen Schutz von Daten und der wirtschaftlichen und wissenschaftlichen Nutzung von Daten findet. Die Schweizer Digitalwirtschaft setzt sich für einen modernen und zweckmässigen Datenschutz ein, der die Innovationskraft des Standorts Schweiz nicht behindert. Ein administrativ tragbares Vorgehen im Rahmen der internationalen Entwicklungen ist dabei zentral.

Mit dem *revidierten Datenschutzgesetz (resDSG)* wurde im Herbst 2020 ein modernes Gesetz geschaffen, welches das Schutzniveau der *Datenschutz-Grundverordnung der EU (DSGVO)* übernimmt, die Anliegen der Politik und Wirtschaft angemessen berücksichtigt und zahlreiche Verbesserungen gegenüber dem bisherigen Datenschutzgesetz (DSG) beinhaltet. Gerade durch seine Angleichung an die DSGVO wird das neue resDSG für die Schweizer Unternehmen gut umsetzbar. Leider ist man bei der Erarbeitung der Verordnung jedoch von diesem wichtigen Prinzip abgekommen. Eine grosse Menge an Sonderregeln haben als «Swiss Finish» ihren Weg in den *Entwurf zur Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)* gefunden. Die Abweichungen sind weder notwendig noch zweckmässig und führen zu einem enormen Mehraufwand für Schweizer Organisationen.

Zudem wurde der politische Prozess bei der Erarbeitung des E-VDSG nicht ausreichend berücksichtigt. So wurden Regelungen, welche im politischen Prozess um die DSG-Revision im Parlament abgelehnt worden waren, in der E-VDSG wiederbelebt (Art. 16 E-VDSG). Zwar ist der Bundesrat berechtigt, Gesetze durch Verordnungen näher auszuführen (Art. 182 Abs. 2 BV); dabei darf er aber nur «Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher ausführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beitragen» (BGE 141 II 169). Mehrere Regelungen im E-VDSG haben diesen Rahmen klar gesprengt, indem sie einen mit den Bestimmungen im revDSG vergleichbaren Regelungsgehalt aufweisen (z.B. Art. 4, Art. 15 und Art. 16). Es ist nicht Aufgabe der Verwaltung, ein parlamentarisches Gesetz nach Abschluss des Gesetzgebungsprozesses auf dem Verordnungsweg zu verschärfen.

Zusammengefasst: Der vorliegende E-VDSG verschärft wesentliche Punkte des Gesetzes, ist inhaltlich nicht ausreichend präzise und unnötig restriktiv. Statt das revDSG im Sinne von Ausführungsvorschriften zu konkretisieren, sieht die Verordnung eine Reihe von bürokratischen Zusatzvorschriften vor, die keine Grundlage im Gesetz finden.

Eine vernünftige Umsetzung der Datenschutzgesetzgebung ist für die digitale Wirtschaft und damit für die Zukunftsfähigkeit und Innovationskraft des Wirtschaftsstandorts Schweiz entscheidend. Der Bund fördert Digitalisierung umfassend und auf allen Stufen. Folgerichtig sollte er das auch beim Thema Datenschutz tun.

Weiter ist der verschärfte E-VDSG mit Blick auf die von KMU geprägte Struktur der schweizerischen Wirtschaft gravierend. Viele der Vorschriften lassen sich entweder gar nicht (Art. 2 E-VDSG) oder nur mit unverhältnismässigem Aufwand umsetzen. Diese Aussicht ist besonders besorgniserregend, weil viele der Pflichten mit strafrechtlichen Sanktionen (Art. 60ff. revDSG) bedroht sind.

Konsequenz: Aufgrund der oben geschilderten Ausgangslage wird der vorliegende Entwurf von digitalswitzerland abgelehnt. Er stellt keine Grundlage für einen zweckmässigen, zukunftsgerichteten Datenschutz dar.

3 Forderungen und Hauptanliegen

Der E-VDSG und der Erläuterungsbericht müssen unter Respektierung der Kohärenz zum revDSG ausführlich überarbeitet werden. Swiss Finishs und unnötigen Restriktionen sind zu vermeiden. Die Überarbeitung muss unter Einsetzung der notwendigen Ressourcen zeitnah dahingehend erfolgen, dass die Äquivalenz aufrechterhalten werden kann.

Die wichtigsten Kritikpunkte und Forderungen für die Überarbeitung sind aus Sicht von digitalswitzerland folgende:

1) Artikel und Prinzipien, welche im politischen Prozess abgelehnt und aus dem Entwurf zum revDSG gestrichen wurden, sollen nicht durch die VDSG wieder eingeführt werden. So z.B. Art. 16, der eine Informationspflicht einführen möchte, von der man sich im Vernehmlassungsprozess zum revDSG verabschiedet hatte.
2) Zahlreiche Swiss Finishs führen zu zwei Standards für Schweizer Organisationen. Die folgenden Artikel sind dabei besonders gravierend und müssen entweder gestrichen oder dahingehend geändert werden, dass sie keine zusätzlichen, über die DSGVO hinausgehenden, Pflichten beinhalten:
    a. Art. 4 Abs. 1 E-VDSG
    b. Art. 13 Abs. 1 E-VDSG
    c. Art. 15 E-VDSG
    d. Art. 19 E-VDSG
3) Widersprüche wie in Art. 13 E-VDSG müssen unbedingt behoben werden. Der Artikel kreiert eine Inkonsistenz in Bezug auf Art. 19 revDSG, Art. 13f. DSGVO und auch zum bisherigen Gesetz (Art. 14 DSG).
4) Weitere zentrale Änderungsvorschläge beziehen sich auf folgende Artikel:
    a. Art. 3 E-VDSG
    b. Art. 8 E-VDSG
    c. Art. 16 E-VDSG

4 Anpassungsvorschläge und Begründungen im Detail

Im Anhang ab Seite 4 werden ausformulierte Anpassungsvorschläge aufgeführt. Diese sind in Abstimmung mit dem Wirtschaftsdachverband economiesuisse entstanden.

Wir danken Ihnen für die Aufmerksamkeit, die Sie unseren Anliegen entgegenbringen und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Nicolas Bürer
Managing Director digitalswitzerland

Andreas W. Kaelin
Deputy Managing Director digitalswitzerland

Für weitere Auskünfte:
Andreas W. Kaelin, digitalswitzerland | Geschäftsstelle Bern
Tel. +41 31 311 62 45 │ andreas@digitalswitzerland.com

5 Anhang: Anpassungsvorschläge im Detail

Anliegen im Falle einer Weiterführung des bisherigen Entwurfs

Kapitel 1: Allgemeine Bestimmungen

Artikel 1 (Grundsätze)

Antrag:

1. Sachlogische Anpassung beim Begriff «Risiko».
2. Berücksichtigung des Implementierungsaufwands statt der -kosten als Kriterium aufnehmen.
3. Anerkennung eines Umsetzungsermessens des Verantwortlichen.

Begründung:

1. Ein Risiko ergibt sich sachlogisch vorab aus einer potenziellen Verletzung der Datensicherheit für die betroffene Person. Für den Fall des Vorliegens einer solchen potenziellen Verletzung stellt sich nachgelagert die Frage nach der Eintrittswahrscheinlichkeit. Dabei sind die Anforderungen an die Datensicherheit höher, je grösser die Eintrittswahrscheinlichkeit ist. Ohne potenzielle Datensicherheitsverletzung stellt sich umgekehrt die Frage nach der Eintrittswahrscheinlichkeit gar nicht. Die Formulierung in Art. 1 Abs. 1 lit. b E-VDSG ist verwirrend, weil sie diese sachlogisch zwingende Reihenfolge nicht beachtet. Die Formulierung in lit. b ist deshalb richtigerweise umzudrehen.
2. Die Aufführung der Implementierungskosten als Kriterium zur Beurteilung der Angemessenheit von technischen oder organisatorischen Massnahmen (sog. TOM) zur Gewährleistung der Datensicherheit ist unseres Erachtens nicht ausreichend. Neben eigentlichen Implementierungskosten fallen typischerweise auch weitere Aufwendungen an, welche zu berücksichtigen sind – so etwa personelle, zeitliche und organisatorische Aufwendungen. Innerhalb einer Auswahl gleichwertiger angemessener Massnahmen darf der Verantwortliche die kostengünstigere auswählen. Dies ist selbstverständlich, da es sich bereits aus dem allgemeinen Verhältnismässigkeitsprinzip ergibt, wird sinnvollerweise aber dennoch erwähnt.
   Zudem sollte nicht allein auf die Implementierungskosten, sondern generell auf den Implementierungsaufwand, der etwa aus personellen, zeitlichen und organisatorischen Aufwendungen besteht, abgestellt werden.
3. Ob, wann und wie eine Überprüfung der TOM stattfinden soll, muss durch den Verantwortlichen bzw. den Auftragsbearbeitenden selbst entschieden werden. Nur er/sie ist in der Lage, den Besonderheiten des Einzelfalls hinreichend Rechnung zu tragen. Ist die Gefährdung der Rechte von Betroffenen grösser, so ist der zeitliche Abstand bis zur nächsten Prüfung sachlogisch kürzer. Die einseitige Fokussierung auf den zeitlichen Abstand einer Prüfung und die zwingende Verknüpfung einer Prüfpflicht ist somit nicht sachgerecht, unnötig einengend und steht im Widerspruch zum risikobasierten Ansatz. Der Begriff «angemessene Abstände» ist durch «angemessene Weise» zu ersetzen.

Formulierungsvorschlag:
1 Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:
a. […];
b. die verbleibenden ~~Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren~~ potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit
c. […];
d. Implementierungs~~kosten~~aufwand.
2 Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessener~~n~~ ~~Abständen~~ Weise zu überprüfen.

Artikel 2 (Schutzziele)

Antrag:
Der Verordnungstext bringt zu wenig klar zum Ausdruck, dass sich die Notwendigkeit der in Art. 2 E-VDSG aufgeführten Schutzziele nach den in Art. 1 E-VDSG vorgeschriebenen Grundsätzen richtet.

Begründung:
Die in Art. 2 Abs. 2 E-VDSG aufgeführten Schutzziele sind veraltet, zu absolut und zu detailliert geregelt. Entsprechend ihrer abstrakten Formulierung erwecken die Schutzziele zudem fälschlicherweise den Eindruck, dass es sich um absolut zu erreichende Anforderungen handelt. Insofern werden statt Minimalanforderungen fälschlicherweise Maximalanforderungen formuliert.

Im Kern muss es im - hier zu regelnden - Bereich der Datensicherheit um die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit gehen. Eine generelle Dokumentationspflicht ist schon deshalb abzulehnen, weil diese so auch vom Gesetzgeber ausdrücklich abgelehnt worden ist.

Selbst die tatsächlich aufzuführenden Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit haben nur beispielhaften Charakter. Sie müssen namentlich dann nicht umgesetzt werden, wenn die Analyse nach Art. 1 E-VDSG dies nicht gebietet. Die Formulierung in der Verordnung sollte dies deutlich zum Ausdruck bringen. Damit sollen nicht zuletzt auch KMU vor unnötigem administrativem Aufwand bewahrt werden. Die vorgeschlagenen Formulierungen bringen zum Ausdruck, dass die Aufzählung in Art. 2 E-VDSG weder vollständig noch verpflichtend ist. Umgesetzt werden muss nur das, was nach Art. 1 E-VDSG zur Gewährleistung einer angemessenen Datensicherheit notwendig ist. Um dieses Ziel zu erreichen, können jedoch auch Massnahmen zur Anwendung kommen, die in Art. 2 E-VDSG nicht erwähnt sind. Mit den von uns beantragten Anpassungen ist die Liste auch konform mit den Anforderungen von Art. 32 EU-DSGVO. Ohne entsprechende Anpassungen läge demgegenüber ein kontraproduktiver Swiss Finish vor, welcher wegen unnötigen Zusatzaufwendungen und Zusatzrisiken auch die EU-Äquivalenz gefährden würde.

Formulierungsvorschlag
~~Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen~~ Basierend auf den Grundsätzen nach Art. 1 ist insbesondere zu beurteilen, welche der nachfolgenden Schutzziele für Systeme und Dienste in Zusammenhang mit der Bearbeitung von Personendaten in Anwendung des risikobasierten Ansatzes im konkreten Fall anwendbar sind:
a. Vertraulichkeit
b. Integrität
c. Verfügbarkeit
d. Belastbarkeit

Artikel 3 (Protokollierung)

Antrag:
Ersatzlos streichen.

Begründung:
Diese Bestimmung ist in mehrfacher Hinsicht problematisch. Das Parlament hat trotz detaillierter Formulierung der Anforderungen an die Datenschutzfolgenabschätzungen in Art. 22 revDSG bewusst auf eine Protokollierungspflicht verzichtet. Darüber hinaus ergibt sich aus zahlreichen Voten im Parlament ebenso wie aus der finalen Fassung des revDSG mit aller wünschbaren Deutlichkeit, dass das Parlament – auch ausserhalb des Datenschutzrechts – am bewährten prinzipien- und risikobasierten Regulierungsansatz festhalten wollte und –

nicht zuletzt, um unnötigen Aufwand für die zahlreichen KMU zu verhindern – namentlich auf unnötige Formvorschriften verzichten wollte. Dazu gehören neben strikt formulierten Dokumentations- und Protokollierungspflichten u.a. auch strikte Aufbewahrungsfristen (deren Dauer über die E-VDSG verteilt zudem eher zufällig mal kürzer, mal länger geregelt werden). Die Festlegung der geeigneten organisatorischen und technischen Massnahmen (TOM) zur Umsetzung von Pflichten gemäss revDSG muss in Anwendung des im revDSG bewusst gewählten prinzipien- und risikobasierten Ansatzes jedem Verantwortlichen bzw. Auftragsbearbeiter nach vernünftigem Ermessen obliegen, namentlich entsprechend den Kriterien Grösse, Struktur, Komplexität, Risiken und Geschäftsmodell (vgl. schon oben Ziff. A. 1-7). Nach alledem widerspricht die in Art. 3 E-VDSG vorgeschlagene Protokollierungspflicht dem klaren gesetzgeberischen Willen, hat somit keine gesetzliche Grundlage und wäre überdies auch in seinen Wirkungen kontraproduktiv, würden doch in Anwendung dieser Pflicht umfassende Protokolle bzw. Logs über praktisch sämtliche Personendatenflüsse eines Verantwortlichen erstellt. Eine solche Pflicht auf Stufe E-VDSG wäre eine klare Verletzung des im revDSG verankerten Verhältnismässigkeitsprinzips (vgl. namentlich Art. 6 Abs. 2 u. 3 revDSG), mithin dem wohl wichtigsten Grundprinzip für ein funktionierendes Datenschutzsystem. In Anwendung von Art. 3 E-VDSG würden denn auch statt Datenschutzprobleme gelöst, auf widersinnige Weise neue geschaffen. Zuletzt müsste auch der Auftragsbearbeiter protokollieren, der aber u.U. gar nicht weiss, ob eine Folgeabschätzung durchgeführt wurde und was ihr Ergebnis war.

Nach alledem ist Art. 3 E-VDSG konsequenterweise **ersatzlos zu streichen**.

Eventualiter:
Will man wider Erwarten nicht so weit gehen, müsste zumindest die Anforderung «Protokollierung» durch «angemessene Dokumentation» ersetzt werden, sowie in Abs. 4 «Protokolle mindestens 2 Jahre aufzubewahren» durch: «Die Aufbewahrungsfrist muss, sofern eine solche gesetzlich festgelegt ist, abhängig von Dauer und Datenbearbeitung und generell angemessen sein».

Artikel 4 (Bearbeitungsreglement von privaten Personen)

Antrag:
Ersatzlos streichen.

Begründung:
Die Regelung wurde im Wesentlichen aus Art. 11 der geltenden VDSG übernommen. Schon jene Bestimmung blieb aber insofern «toter Buchstabe», als es ein solches «Bearbeitungsreglement» in dieser Form in der operativen Praxis von Unternehmen nicht gibt. Vielmehr werden die zahlreichen notwendigen Regelungen gemäss bewährter Usanz in einem ganzen Paket von sich gegenseitig ergänzenden Weisungen samt dazugehörigen Prozessen und Listen mit Aufgaben, Kompetenzträgern und Verantwortlichkeiten abgebildet. Diese sind sehr viel wirkungsvoller als ein starres Reglement. Das in der E-VDSG vorgesehene Bearbeitungsreglement kann die immer komplexeren Datenbearbeitungen in der Praxis nicht mehr sinnvoll abbilden. Diese Aufgabe übernimmt zu Recht das neu zu führende Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG).

Umso unverständlicher ist, dass die Regelung von Art. 4 E-VDSG weitgehend deckungsgleich mit den Anforderungen an das gemäss Art. 12 revDSG zu erstellenden Verzeichnis der Bearbeitungstätigkeiten ist, was unnötigerweise Rechtsunsicherheit und unnötigen Doppelaufwand produziert. Das revDSG sieht in Art. 12 bereits vor, dass die Datenverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen müssen. Dieses muss ähnliche Informationen enthalten wie das Bearbeitungsreglement. Mit der Einführung des Verzeichnisses macht ein zusätzliches Bearbeitungsreglement keinen Sinn, zumal dieses weitgehend die gleichen Informationen enthält.

Die Aufgreifkriterien gemäss Art. 4 Abs. 1 E-VDSG sind keineswegs klar abgrenzbar. Im Bereich Profiling besteht unter Würdigung sämtlicher Kriterien ein gewisses Ermessen, wann die Grenze zu «hohem Risiko» erreicht ist. Die gesetzliche Regelung (vgl. Art. 5 lit. f und g revDSG) gibt hierzu auch keine klaren Vorgaben, weil nur technische Beschreibungen ohne echte Abgrenzungskriterien festgelegt wurden. Namentlich wiederholt die Regelung für Profiling mit hohem Risiko (Art. 5 lit. g revDSG) im Kern einen technischen Beschrieb, welcher auf jedes Profiling zutrifft und lässt offen, wann die Grenze zu einem «hohen Risiko» erreicht ist. Kritisch ist auch das Aufgreifkriterium «Bearbeitung umfangreicher besonders schützenswerter Personendaten» gemäss Art. 4 Abs. 2 Abs. 1 lit. b E-VDSG. Dies dürfte bei HR-Daten rasch der Fall sein, auch bei den KMU. Die offene Formulierung «umfangreich» ist deshalb als Aufgreifkriterium nicht geeignet. Nach alledem müssten sorgfältige Verantwortliche im Zweifelsfall einen Grossteil ihrer Datenbearbeitungen den Regeln von Art. 4 E-VDSG unterstellen. Gemäss Systematik von Art. 4 Abs. 1 E-VDSG ist dies aber gar nicht beabsichtigt, soll doch Art. 4 E-VDSG nur auf Ausnahmen von der Regel anwendbar sein. Diese misslungene Regelung ist ein eigenständiger Grund für die ersatzlose Streichung von Art. 4 E-VDSG.

Auch hat ein Bearbeitungsreglement mit der Datensicherheit im eigentlichen Sinne, die Art. 8 Abs. 3 revDSG regelt, nicht zu tun. Es fehlt daher die gesetzliche Grundlage für eine Pflicht, ein Bearbeitungsreglement zu führen.

Art. 4 E-VDSG generiert somit statt Klärung bloss Verwirrung und unnötige Abgrenzungsprobleme. Zwei weitgehend deckungsgleiche Regelungen zu erlassen, ist gänzlich sinnlos. Dies umso mehr, als die meisten Schweizer Unternehmen überdies auch grenzüberschreitende Geschäfte betreiben und deshalb entsprechende Verzeichnisse nicht nur nach dem revDSG, sondern überdies auch nach der EU-DSGVO erarbeiten müssen.

Demzufolge ist Art. 4 E-VDSG **ersatzlos zu streichen**.

Artikel 6 (Modalitäten)

Antrag:

1. Klarstellung im Erläuterungsbericht, dass die VDSG – anders als die DSGVO – keinen Mindestinhalt an den Auftragsdatenverarbeitungsvertrags (ADV) vorschreibt.
2. Streichung von Abs. 1
3. Streichung von Abs. 2

Begründung:

1. Es ist unklar, was die Ausführungen auf S. 24 der Erläuterungen zu den Anforderungen an den Inhalt des ADV gemäss Art. 22 Abs. 3 DSGVO bezwecken, zumal diese in Art. 6 E-VDSG nicht vorgesehen sind. Diese Ausführungen suggerieren, dass der ADV gemäss Art. 6 VDSG den inhaltlichen Anforderungen der DSGVO genügen müsse. Hierfür findet sich indes keine gesetzliche Grundlage. Auch die E-VDSG enthält keine inhaltlichen Vorgaben.
2. Absatz 1 wiederholt zuerst eine Banalität und ist gleichzeitig ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann, wenn ihm nichts vorgeworfen werden kann. Dem sollte nicht so sein. Es ist ohnehin nicht klar, was mit «für den Datenschutz verantwortlich» gemeint ist. Strafrechtliche Verantwortlichkeit kann es nicht sein und aufsichtsrechtliche Verantwortlichkeit setzt ebenfalls Kontrollmöglichkeiten voraus. Wird die Verantwortlichkeit schliesslich als zivilrechtliche Haftung verstanden, dann wird mit dieser Regelung eine vom Gesetzgeber nicht vorgesehene Kausalhaftung eingeführt. Hierfür fehlt eine gesetzliche Grundlage. Dies würde auch

über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Zudem ist die Formulierung «sicherstellen» inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen».
Auch dem zweiten Satz fehlt eine gesetzliche Grundlage. Nach Art. 9 Abs. 1 lit. a revDSG hat der Verantwortliche dafür zu sorgen, dass die Daten so bearbeitet werden, wie er es selbst darf. Nach Satz 2 hat er jedoch auch für die Durchsetzung seines eigenen Vertrags zu sorgen, selbst wenn dieser strenger sein sollte als das Gesetz. Macht er also einen zu strengen Vertrag, erlaubt aber seinem Auftragsbearbeiter eine Bearbeitung, die dem noch Gesetz entspricht, ist diese Vorschrift bereits verletzt. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 lit. a revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das sollte genug Schutz bieten, sodass die Regelung hier obsolet wird.

3. Der Sinn und Zweck der Regelung von Abs. 2 erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) abgedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt es sich aber um eine Bestimmung für Bundesorgane, während Art. 6 Abs. 2 E-VDSG sowohl für Datenbearbeitungen Privater als auch für solche von Bundesorganen gelten soll. Aus dem Erläuterungsbericht geht nicht hervor, warum diese Bestimmung nun auch für Private gelten soll. Offen bleibt auch, weshalb es die Regelung überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt.
   Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter einsetzt, um Daten zu bearbeiten, ohne dass es zu einer Bekanntgabe aus der Schweiz kommt und somit Art. 16 revDSG nicht greift. Systematisch wäre aber auch dieser Fall in Art. 16 revDSG zu regeln und nicht in der VDSG. Zudem ist diese Konstellation ein absoluter Sonderfall. Eine eigene Regelung in der E-VDSG rechtfechtfertigt sich somit nicht. Die Regelung ergibt sich im Übrigen ohnehin bereits aus Art. 9 Abs. 1 lit. a revDSG, und zwar systematisch korrekt, während sie hier systematisch falsch angelegt ist: Im Falle einer Auftragsbearbeitung geht es um die Sicherstellung eines gleichwertigen Datenschutzes, da der Auftragsbearbeiter die Daten gar nicht in eigener Regie bearbeiten darf. Vielmehr geht es darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 lit. a revDSG.

Aufgrund obiger Ausführungen sind Art. 6 Abs. 1 sowie Abs. 2 E-VDSG **ersatzlos zu streichen**.

Artikel 8 (Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs)

Antrag:
Sowohl in Abs. 1 als auch in Abs. 3 und 6 braucht es eine Anpassung, um klarzustellen, dass sich die Regelung nur an den Bundesrat richtet.

Begründung:
Nach Art. 16 Abs. 1 revDSG legt nunmehr der Bundesrat fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten.

Der Wortlaut von Art. 8 Abs. 1 und 6 E-VDSG kann dahingehend missverstanden werden, dass die verantwortliche Stelle – und nicht der Bundesrat – die Angemessenheit des Datenschutzes in einem Empfängerstaat feststellen muss. Somit muss klargestellt werden:

- dass sich dieser Artikel nur an den Bundesrat (BR) richtet;
- dass der BR einzige kompetente Stelle wird, welche eine solche Positiv-Liste erlassen kann – der EDÖB wird vom BR konsultiert, kann jedoch keine eigene Liste herausgeben. Die Aufgabe des EDÖB liegt neu

lediglich darin, Empfehlungen/Assessmentvorgaben für den Datentransfer in Länder zu formulieren, die nicht auf der Positiv-Liste sind;
- dass die Positiv-Liste des BR verbindlich ist.

Formulierungsvorschlag:
1 Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~ muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:
[…]
6 Der Bundesrat konsultiert den EDÖB ~~wird~~ vor jedem Entscheid über die Angemessenheit des Datenschutzes ~~konsultiert~~.

Implikationen als Folge der Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Rechtssache Schrems II sowie des Positionspapiers und der Handlungsanleitung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in gleicher Sache (Art. 8 Abs. 1 Satz 2 E-VDSG und Abs. 7 E-VDSG).

Wie bereits erwähnt, legt nunmehr der Bundesrat fest, welche Staaten oder internationale Organe einen angemessenen Datenschutz gewährleisten. Gemäss dem erläuternden Bericht des Bundesamtes für Justiz soll daher die Verordnung neu die Kriterien regeln, welche der Bundesrat bei seinem Entscheid berücksichtigt. In Anhang 1 sind tabellarisch diejenigen Staaten und internationalen Organe aufgeführt, welche über ein angemessenes Datenschutzniveau verfügen.

Der Bundesrat erstellt die Liste der Länder mit angemessenem Datenschutz nach bestem Wissen und Gewissen. Die Verantwortlichen dürfen sich auf diese Liste im Prinzip verlassen und müssen nicht per se eigene Abklärungen vornehmen, welche die Einschätzung des Bundesrates bestätigen. Die Liste geniesst aber keinen öffentlichen Glauben (anders als z.B. das Grundbuch). Die Verantwortlichen dürfen sich deshalb nur so lange auf Gutgläubigkeit berufen und sich auf die Liste verlassen, wie ihnen aus eigener Erfahrung nichts Gegenteiliges bekannt ist. Ohne dahingehenden eigenständigen Verdachtsanlass selbst Abklärungen über die Richtigkeit der Liste vornehmen muss der Verantwortliche aber nicht (vgl. schon BJ-Erläuterungen zum DSG vom 24. März 2006, S. 8, Antwort zu Frage 49).

Am 18. Juni 2021 hat der EDÖB eine Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug veröffentlicht. Soweit danach ein Land auf der Staatenliste (des EDÖB und künftig des Bundesrates) fehlt oder mit einem ungenügenden Schutzniveau ausgewiesen ist, muss der Datenexporteur prüfen, ob kumulativ folgende vier Garantien eingehalten werden:

- klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden;
- Verhältnismässigkeit der behördlichen Befugnisse und Massnahmen;
- wirksame, gesetzlich verankerte Rechtsbehelfe für die Durchsetzung von Rechten von Betroffenen in der Schweiz;
- Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht.

Erfüllt das lokale Recht die genannten Garantien nicht, muss der Datenexporteur weitere technische, organisatorische und rechtliche Massahmen treffen. Kann durch solche Massnahmen der fehlende Schutz nicht ausgeglichen werden, folgt daraus, dass die Datenbekanntgabe ins Ausland ausgesetzt bzw. beendet wird.

Nach der Handlungsanleitung des EDÖB soll der Datenexporteur als gutgläubig gemäss Art. 3 Abs. 1 ZGB gelten, soweit er Daten in einen Staat übermittelt, der auf der Staatenliste als ein solcher mit angemessenem Datenschutzniveau aufgeführt wird. Hierbei soll es sich allerdings um eine widerlegbare Vermutung handeln. So soll der verantwortliche Datenexporteur bei der Erfassung und Analyse des Datentransfers alle nötigen Abklärungen vornehmen müssen, wie z.B. Einholen von unabhängigen Rechtsgutachten, u.a. zu folgenden Aspekten:

- Geltende Rechtsvorschriften im Zielland;
- Praxis der Verwaltungsbehörden und Gerichtsbehörden;
- Rechtsprechung.

Verbindlichkeit des Entscheids des Bundesrats zur Angemessenheit des Datenschutzes (Klarstellung in Art. 8 Abs. 1 Satz 2 E-VDSG)

Die durch den EDÖB vorgeschlagene Prüfung der obenstehenden Garantien durch den Datenexporteur muss sich aufgrund einer positiven Entscheidung des Bundesrats hinsichtlich der Angemessenheit des Datenschutzes in einem Drittstaat erübrigen. Dies folgt bereits daraus, dass ohne die Vorlage solcher Garantien nicht von einem angemessenen Datenschutz ausgegangen werden kann.

Eine zusätzliche Einzelfallprüfung und die damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates, hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur, erscheint darüber hinaus aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Denn einerseits sind die relevanten Rechtsgrundlagen, Rechtsprechung sowie insbesondere die Behördenpraxis für (geheime) Zugriffe nicht einheitlich kodifiziert und/oder öffentlich zugänglich. Der Bundesrat und speziell das EDA und das EJPD verfügen hier über die besten Quellen und Kenntnisse. Andererseits wäre eine solche Beurteilung als unverhältnismässig aufwändig zu werten, da diese eine Momentaufnahme widerspiegelt, die einem raschen Wandel unterliegen kann. Folglich könnte ein Verantwortlicher gar nicht innert vertretbarer Zeit adäquat auf Änderungen reagieren und sofortige neue Dispositionen treffen.

Darüber hinaus würde der Umstand, Unternehmen als Datenexporteure mit der Aufgabe zu betrauen, die Angemessenheit der Rechtsordnungen des Importstaates zu untersuchen und zu beurteilen, Art. 16 revDSG i.V.m. Art. 8 E-VDSG widersprechen. Diese Normen legen fest, dass die Angemessenheitsprüfung und die damit einhergehende Entscheidung vom Bundesrat und nicht von den datenexportierenden Stellen vorgenommen werden muss. Sollte nicht einheitlich der Bundesrat, sondern die datenexportierenden Verantwortlichen solche Beurteilungen vornehmen, sind unterschiedliche Ergebnisse hinsichtlich bestimmter Länder und Datenverarbeitungen vorprogrammiert. Dies würde im Ergebnis trotz viel Aufwand keine Rechtssicherheit schaffen. Die Liste des Bundesrats verlöre dadurch jeden Sinn.

Um eine faktische Aushöhlung der Feststellungskompetenz des Bundesrates sowie unterschiedliche Ergebnisse der Bewertung und eine damit einhergehende Rechtsunsicherheit zu vermeiden, muss deshalb auf Stufe E-VDSG ausdrücklich geklärt werden, dass sich die Verantwortlichen als Datenexporteure auf den Entscheid des Bundesrates zur Angemessenheit verlassen dürfen und keine zusätzlichen Abklärungen treffen müssen.

Daher soll zur Klarstellung **ein neuer Satz 2 in Art. 8 Abs. 1** E-VDSG eingefügt werden.

Formulierungsvorschlag
1 Werden Personendaten ins Ausland bekanntgegeben, so ~~müssen~~ muss der Bundesrat bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigen~~t werden~~:
(a-~~e~~) …
Die Verantwortlichen dürfen sich auf den Entscheid des Bundesrates zur Angemessenheit des Datenschutzes nach Satz 1 verlassen und müssen keine zusätzlichen Abklärungen treffen.

Staaten oder internationale Organe ohne angemessenen Datenschutz (Klarstellung in Art. 8 Abs. 7 E-VDSG)

Alle nicht auf der Liste des Bundesrates aufgeführten Länder gelten per se als Länder mit nicht angemessenem Datenschutz. Wollen Verantwortliche in solche Länder Personendaten versenden bzw. dort bearbeiten (lassen), müssen sie selbst abklären, ob ein angemessener Datenschutz gegeben ist oder andernfalls ergänzend geeignete und angemessene Zusatzmassnahmen treffen. Das Urteil Schrems II des EuGHs generiert entgegen den Leitlinien des EDÖB vom 18. Juni 2021 in diesem Zusammenhang keine zusätzliche Liste von Ländern mit besonderem Risiko. Dies schon deshalb, weil sachlogisch bei jedem Land mit nicht angemessenem Datenschutz damit zu rechnen ist, dass spezifische Behörden und Stellen wie z.B. Geheimdienste ungefragt Einsicht in die betreffenden Daten nehmen und deshalb auch vom Urteil Schrems II erfasst sind. Eine solche Liste von Ländern mit hochgradig nicht angemessenem Datenschutz dürfte auch aus politischen Gründen nicht opportun sein, da sie wichtige internationale Beziehungen der Schweiz nachhaltig gefährden dürfte. Dies ist in Art. 8 E-VDSG im Sinne einer notwendigen Präzisierung klarzustellen, um obgenannte Leitlinien des EDÖB zu entkräften, sachlogisch in einem neuen Abs. 7.

Sollte an der durch den EDÖB vorgeschlagenen zusätzlichen Prüfung der obenstehenden Garantien, welche aus einer entsprechenden Auslegung der Schrems-II-Rechtsprechung des EuGHs resultiert, festgehalten werden, müsste die Prüfung dieser Garantien sachlogisch ebenfalls einheitlich durch den Bundesrat erfolgen. Dies auch deshalb, weil die Abgrenzung zwischen «nicht angemessen» und «hochgradig nicht angemessen» zwingend Wertungen beinhaltet, welche gesamthaft einheitlich von einer kompetenten Stelle anzuwenden sind. Nur dadurch wird ein in sich stimmiges Regelungssystem für die gesamte Thematik geschaffen, welches statt Verwirrung tatsächlich Rechtssicherheit schaffen würde. Andernfalls ergäben sich kontraproduktive Widersprüche zwischen der Liste des Bundesrates und den Zusatzlisten der Verantwortlichen. Als Folge davon würde die bereits vorstehend skizzierte Rechtsicherheit (oben Ziff. 2.2) trotz viel Aufwand sogar noch weiter erhöht.

Eine Einzelfallprüfung und eine damit einhergehende Beurteilung und Entscheidung zur jeweiligen (ausländischen) Rechtsordnung des Importstaates hinsichtlich hinreichender Transparenz und Rechtsschutz für die betroffenen Personen durch den Datenexporteur erscheint aus Praktikabilitätsgründen weder als durchführbar noch als zielführend.

Nach alledem ist zur Klarstellung ein **neuer Absatz 7 in Art. 8 E-VDSG** einzufügen.

Formulierungsvorschlag
[…]
7) Werden Personendaten ins Ausland in einen Staat oder ein Gebiet ohne angemessenen Datenschutz bekanntgegeben, können ergänzende Massnahmen zu den Garantien gemäss Art. 16 Absatz 2 Buchstabe b und c DSG erforderlich sein, um einen geeigneten Datenschutz zu gewährleisten. Der Bundesrat stellt fest, ob ergänzende Massnahmen erforderlich sind. Die betroffenen Staaten und Gebiete sind im Anhang 1a aufgeführt. Der Entscheid des Bundesrates bezüglich der Erforderlichkeit ergänzender Massnahmen ist verbindlich.

Artikel 9 (Datenschutzklauseln und spezifische Garantien)

Antrag:
Zumindest Abs. 1 lit. d, e, f, h und j sollen gestrichen werden. Lit. a soll um den Grundsatz der Transparenz ergänzt und in lit. g muss der «berechtigte Empfänger» durch den «Empfänger» ersetzt werden.

Begründung:

- Die von Art. 9 E-VDSG gestellten Anforderungen sind nicht erforderlich. Der EDÖB muss sie ohnehin prüfen. Zudem erreichen sie ein Detaillierungsniveau, welches die Komplexität der Datenbearbeitung unnötig erhöht. Zwar sind diese Anforderungen für das Ziel des Datenschutzes konsequent, sie verursachen aber hohe Bearbeitungskosten für involvierte Betriebe. Deswegen sollten diese Anforderungen auf das Minimum reduziert werden.
- In den Bearbeitungsgrundsätzen (lit. a) fehlt der Grundsatz der Transparenz.
- Das Erfordernis in lit. d und e, den Namen der Staaten oder der internationalen Organisationen zu nennen, denen Personendaten bekanntgegeben werden (soweit hiermit Weiterübermittlungen gemeint sind, was nicht klar ist), hat keine rechtliche Grundlage. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf.
- Lit. f ist bereits mit dem Grundsatz der Verhältnismässigkeit in lit. a abgedeckt, und damit redundant und zu streichen.
- Lit. g geht zu weit, indem es die «berechtigten» Empfänger verlangt. Relevant sind die «Empfänger», also normalerweise die Parteien, welche den Vertrag abschliessen und damit bereits ersichtlich sind.
- Lit. h ist klarerweise unnötig und seine Anwendung wäre unverhältnismässig aufwendig. Andere bestehende Bestimmungen genügen, um die Garantien zu sichern und einen angemessenen Schutz bei der Lieferung von Daten ins Ausland zu gewährleisten.
- In Abs. 2 sollte die Datenschutzklausel die Pflicht des Empfängers enthalten, die betroffenen Personen zu informieren. Es ist nicht Aufgabe des Auftragsverarbeiters, die betroffenen Personen zu informieren; dies ist Aufgabe des Verantwortlichen.

Aus diesen Ausführungen folgt überdies, dass der Anforderungskatalog in Art. 9 Abs. 1 E-VDSG entweder anzupassen ist, um unterschiedliche Konstellationen abzudecken (Verantwortlicher, Auftragsbearbeiter) und das Wort «mindestens» durch «je nach den Umständen» zu ersetzen ist.

Das DSG schreibt – wie die DSGVO – kein proaktives «Sicherstellen» der Einhaltung der Garantien durch den Verantwortlichen vor. Ein Eingreifen in Fällen, in welchen ein solches «Nicht-Einhalten» und damit eine Verletzung der Vertragspflichten eintritt, ist jedoch eine Reaktion durch den Verantwortlichen selbstverständlich, und kann entsprechend auch in Art. 9 Abs. 2 in die Verordnung aufgenommen werden.

Demnach ist Art. 9 E-VDSG wie folgt anzupassen:

Formulierungsvorschlag:
1) Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen je nach den Umständen ~~mindestens die~~ folgende~~n~~ Punkte regeln:
a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung, ~~und~~ der Richtigkeit und der Transparenz;
b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
c. die Art und den Zweck der Bekanntgabe von Personendaten
~~d. die Namen der Staaten, in die Personendaten bekanntgegeben werden;~~
~~e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden;~~
~~f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;~~
g. die Modalitäten der Weitergabe von ~~zur Bearbeitung der~~ Daten ~~berechtigten~~ an Empfängerinnen und Empfänger;
~~h. die Massnahmen zur Gewährleistung der Datensicherheit;~~
i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;
~~j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren;~~
k. […]
2) Der Verantwortliche muss angemessene Massnahmen treffen, ~~um sicherzustellen, dass~~ wenn die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien nicht einhält
3) […]

Artikel 10 (Standarddatenschutzklauseln)

Antrag:
Der Empfänger kann nicht verpflichtet werden, «die schweizerischen Datenschutzvorschriften» einzuhalten. Das ist im Erläuterungsbericht klarzustellen.
Und
Ersetzen des Begriffs «Sicherstellung» durch «darauf hinwirken».
Und
Präzisierung, dass sich die Angemessenheit der geforderten Massnahmen nach den Umständen im konkreten Einzelfall richte und die Anforderungen insb. dann höher seien, wenn es sich um besonders schützenswerte Personendaten handle.

Begründung:
Im Erläuterungsbericht (S. 28) ist festgehalten, dass der Empfänger verpflichtet werden müsse, «die schweizerischen Datenschutzvorschriften» einzuhalten. Das ist unzutreffend; er muss die Standardklauseln einhalten, nicht jedoch das Schweizer Datenschutzrecht. So verlangt auch Art. 6 Abs. 2, dass der Auftragsbearbeiter «gleichwertige» Bestimmungen einhalten muss.

Der Exporteur kann nicht «sicherstellen», dass der Empfänger die Standarddatenschutzklauseln beachtet; er kann nur, aber immerhin, darauf hinwirken.

Dies ist in den Erläuterungen (S. 28) unter Hinweis auf das BJ entsprechend festgehalten und sollte zur Klarstellung auch in die Verordnung einfliessen.

Der risikobasierte Ansatz bei der Beurteilung von Datentransfers in Länder ohne angemessenen Datenschutz auf Grundlage der SCC ist zu bejahen. Allerdings ist dieser Ansatz mit Blick auf die Praxishinweise der EU-Behörden keinesfalls selbstverständlich. Entsprechend bedarf es einer Klarstellung in der Verordnung zur Schaffung von Rechtssicherheit.

Formulierungsvorschlag:
1 Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Abs. 2 Buchstabe d DSG ins Ausland bekannt, so ~~trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.~~ trägt er in angemessener Weise Sorge für deren Einhaltung.

Und
Klarstellung im Erläuterungsbericht, dass der Empfänger nicht verpflichtet werden muss, «die schweizerischen Datenschutzvorschriften» einzuhalten.

2. Kapitel: Pflichten der Verantwortlichen ~~und des Auftragsbearbeiters~~

Da die Pflichten des Auftragsbearbeiters aus Sicht der Wirtschaft dringend gestrichen werden sollten, muss der Titel von Kapitel 2 angepasst werden.

Artikel 13 (Modalitäten der Informationspflicht)

Antrag:
1. Streichung des Auftragsverarbeiters.

Und
2. Ergänzung der Möglichkeit eine Information auch elektronisch zur Verfügung zu stellen.

Und
3. Streichung der unpräzisen Vorgaben für eine angemessene Information und Streichung der unklaren Anforderungen an Piktogramme.

Begründung:
1. Die Informationspflicht gegenüber den betroffenen Personen kann nur den Verantwortlichen treffen. Die vorgeschlagene Regelung steht im diametralen Widerspruch zum neuen DSG (Art. 19 revDSG) (!) und der DSGVO (Art. 13 und 14). In beiden Gesetzen trifft die Informationspflicht – selbstverständlich - nur den Verantwortlichen. Der Auftragsbearbeiter muss und kann nicht informieren, und er darf es auch gar nicht, ausser auf Weisung und in Vertretung des Verantwortlichen. Im Übrigen ist diese Pflicht strafbewehrt (Art. 60 revDSG), so dass auf diesem Weg auch die Strafbarkeit des Auftragsverarbeiters bzw. der für ihn handelnden Personen eingeführt würde. Dafür bräuchte es aus rechtstaatlichen Gründen zwingend ein Gesetz im formellen Sinn, was die VDSG nicht ist.
   Es ist zudem falsch, dass die Pflichtangaben «mitzuteilen» sind. Es geht bei der Datenschutzinformation nicht um eine Mitteilung wie bei bestimmten rechtgeschäftlichen Erklärungen, die dem Empfänger zugehen müssen (vgl. z.B. Art, 40e Abs. 4, Art. 176 Abs. 2 oder Art. 269d OR), sondern darum, eine bestimmte Situation – die Bearbeitung – nach aussen erkennbar zu machen. Vergleichbar ist dies mit der Deklaration von Konsumenteninformationen (vgl. Art. 1 lit. a KIG). Bei Art. 13 Abs. 1 E-VDSG ist deshalb von «zur Verfügung stellen» zu sprechen anstelle von «mitteilen».
2. Das revDSG sieht nicht vor, dass die Betroffenen die «wichtigsten Informationen» auf der «ersten Kommunikationsstufe» erhalten müssen (vgl. aber Erläuterungen, S. 30). Vielmehr hält revDSG Art. 19 Abs. 1 fest, die Information müsse «angemessen» erfolgen. Daraus folgt, dass die Mitteilung von den jeweiligen Umständen abhängig ist. Dabei sind auch Informationsinteresse und die Erwartungen des Betroffenen zu

berücksichtigen: Während er damit rechnen mag, dass sich in einem Vertrag ein Hinweis auf die Datenschutzerklärung findet, ist ein solcher auf Visitenkarten, E-Mails oder Briefpapier nicht üblich. Sollte sich eine Person ausnahmsweise dafür interessieren, kann ihr ohne weiteres zugemutet werden, z.B. die Webseite des betreffenden Unternehmens zu konsultieren. Darum darf es nicht erforderlich sein, in Alltagssituationen – wie bei einer Terminvereinbarung am Schalter – explizit auf die Datenschutzerklärung hinweisen zu müssen. Dabei ist der Standard «auf Papier oder elektronisch zur Verfügung stellen» zu wählen, welcher in neueren Gesetzen wie z.B. FIDLEG bereits genutzt wurde. Zudem wäre ohnehin unklar, welches die «wichtigsten Informationen» sind.

3. Weil Piktogramme ohnehin nur ergänzend verwendet werden dürfen, sind daran keine zusätzlichen Anforderungen zu stellen. Zumal aufgrund der Erläuterungen nicht klar ist, was mit «maschinenlesbar» gemeint ist.

Formulierungsvorschlag
1. Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~ stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form ~~mit~~ auf Papier oder elektronisch zur Verfügung.
2. ~~Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~

Artikel 15 (Information bei der Bekanntgabe von Personendaten)

Antrag:
Ersatzlos streichen.

Begründung:
Art. 15 E-VDSG statuiert völlig neue formale zusätzliche Modalitäten und Zusatzpflichten in Zusammenhang mit der Bekanntgabe von Daten an Dritte, welche strikt regelbasiert ohne Differenzierungsmöglichkeit in jedem Fall anwendbar sein sollen. Hierzu findet sich im revDSG keine gesetzliche Grundlage. Im Gegenteil hat das Parlament die Bekanntgabe von Personendaten an Dritte bereits auf Gesetzesstufe an verschiedenen Stellen ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt (vgl. namentlich Art. 16 ff. revDSG). Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.

Die Regelung würde inhaltlich zu massiven Zusatzanforderungen bei jeder Art von Kommunikation in Zusammenhang mit Personendaten, z.B. bei jedem einzelnen E-Mail, führen. Damit würden an übliche und vernünftige Kommunikation, selbst solche ohne erkennbare datenschutzrechtliche Risiken, völlig überrissene Anforderungen gestellt. Im operativen Alltag würden damit etablierte, übliche und vernünftige Kommunikationsmittel wie z.B. E-Mail de facto gänzlich verhindert. Solche Anforderungen stehen in vollständigem Widerspruch zu den Anstrengungen des Bundesrats, Digitalisierung und Innovationskraft im Interesse des Wirtschaftsstandorts Schweiz zu fördern.

Dementsprechend finden sich auch im EU-Recht, auf welches sich der Erläuterungsbericht zu Unrecht beruft, keine solchen Pflichten für private Datenbearbeiter. Art. 15 E-VDSG ist mithin ein für das wesentliche Regulierungsziel EU-Äquivalenz kontraproduktiver Swiss Finish.

Somit ist die Regelung Art. 15 **am besten gänzlich zu streichen, zumindest** aber ausdrücklich **auf Bundesorgane einzugrenzen**.

Sofern die Regelung nicht gänzlich gestrichen wird, ist zudem auch hier der Auftragsbearbeiter jedenfalls nicht Adressat der Informationspflicht und ist deshalb zu streichen. Der Auftragsbearbeiter verfügt weder über die entsprechenden Angaben noch ist er zu einer solchen Mitteilung befugt, es sei denn auf Weisung und in Vertretung des Verantwortlichen.

Artikel 16 (Information über die Berichtigung, Löschung und Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten)

Antrag:
Ersatzlos streichen.

Begründung:
Die Pflicht wurde im Rahmen der Vernehmlassung zum revDSG gestrichen und darf nun nicht über die VDSG wieder eingeführt werden. Zudem besteht keine Notwendigkeit, da der Verantwortliche bei der Datenbearbeitung ohnehin die Bearbeitungsgrundsätze einzuhalten hat, ebenso wie die Empfänger von Personendaten.

Darum ist Art. 16 E-VDSG **zu streichen**.

Artikel 17 (Überprüfung einer automatisierten Einzelentscheidung)

Antrag:
Ersatzlos streichen.

Begründung:
Dieser Artikel stellt unseres Erachtens einen Eingriff in die Privatrechtsautonomie dar und kann daher nicht auf Verordnungsstufe verankert werden.

Zudem geht die Regelung von falschen rechtlichen Voraussetzungen aus. Ein generelles Diskriminierungsverbot gibt es nicht. Soweit es direkt aus Grundrechten der Verfassung abgeleitet werden sollte, wäre dies unzulässig, da es keine direkte Drittwirkung verfassungsmässiger Rechte gibt. Eine Diskriminierung wird rechtlich erst dann kritisch, wenn sie rein subjektiv ohne sachlich überzeugende Abgrenzungskriterien erfolgt. All dies ist aber schon deshalb nicht auf Stufe E-VDSG zu regeln, weil das Thema allgemeiner Natur ist und in sämtlichen Rechtsmaterien gleichermassen eine Rolle spielt. Nur schon die etablierte bundesgerichtliche Praxis zum Thema gibt ausreichende Rechtssicherheit.

Eine weitere Präzisierung von Art. 21 revDSG auf Stufe E-VDSG ist weder sinnvoll noch nötig und mangels gesetzlicher Grundlage auch nicht zulässig. Das Parlament hat die Anforderungen an die Informationspflichten bei automatisierten Einzelentscheiden in Art. 21 revDSG bereits ausreichend klar, aber gleichwohl prinzipien- und risikobasiert geregelt. Dementsprechend will das Parlament darüber hinaus bewusst einen angemessenen Ermessensspielraum für die individuelle Umsetzung durch den einzelnen Verantwortlichen zur Verfügung stellen.

Nach alledem gleichwohl eine solche Regel in die E-VDSG einzuführen würde unnötigerweise erhebliches Potential für missbräuchliche Klagen gegen Verantwortliche produzieren, welche sich effektiv absolut korrekt und gesetzeskonform verhalten.

Art. 17 E-VDSG sollte demnach **ersatzlos gestrichen werden**.

Artikel 18 (Form und Aufbewahrung der Datenschutz – Folgeabschätzung)

Antrag:
Die Aufbewahrungsfrist ist zu streichen und «schriftlich» zu präzisieren.

Begründung:
Wie in anderen modernen Gesetzen auch sollte der Begriff der Schriftlichkeit dahingehend präzisiert werden, dass auch andere Formen erfasst werden, die den Nachweis durch Text ermöglichen.

Die Aufbewahrungspflicht sollte im zweiten Satz von Art. 18 E-VDSG mangels gesetzlicher Grundlage im revDSG gestrichen werden. Ausserdem besteht unseres Erachtens aufgrund des Grundsatzes der Verhältnismässigkeit der Datenbearbeitung sowie der Datenminimierung kein Grund, eine Datenschutz-Folgenabschätzung während zwei Jahren nach Beendigung der Datenbearbeitung aufzubewahren. Schliesslich widersprechen die Ausführungen im Erläuterungsbericht dem nemo-tenetur-Grundsatz, sollten die Datenschutz-Folgenabschätzung zu Beweiszwecken gegen den Verantwortlichen aufbewahrt werden.

Sollte an den zwei Jahren festgehalten werden, müsste mindestens die Ergänzung «während mindestens zwei Jahren» oder «für einen angemessenen Zeitraum» eingesetzt werden, sodass eine allfällige längere Aufbewahrung der Daten nicht als datenschutzwidrig gilt.

Formulierungsvorschlag:
1 Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder in anderer durch Text nachweisbarer Form festhalten. ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~

Artikel 19 (Meldung von Verletzungen der Datensicherheit)

Antrag:

1. Lit. e und lit. f sind zu präzisieren.
2. Streichung der über das Gesetz hinausgehenden generellen Pflicht, die betroffene Person zu informieren.
3. Streichung der gesetzlich nicht vorgesehenen Dokumentationspflicht nach VDSG Art. 19 Abs. 5.
4. Anpassung Erläuterungsbericht: Die Auslegung des Begriffs «voraussichtlich» ist falsch und zu korrigieren.

Begründung:

1. Lit. e ist falsch formuliert. Die «allfälligen Risiken» beinhalten bereits die Folgen für die betroffenen Personen. Richtig müsste es heissen: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in lit. f muss nicht von den «Folgen», sondern vom «Risiko» die Rede sein. Gemildert werden kann entweder das Schadensausmass oder dessen Eintrittswahrscheinlichkeit oder beides (was somit dem «Risiko» entspricht). Bei Bst. f ist zudem zu präzisieren, dass es nur um Massnahmen gehen kann, welche der Verantwortliche tatsächlich ergriff («gegebenenfalls»).
2. Art. 19 Abs. 2 E-VDSG geht über Art. 20 Abs. 4 revDSG hinaus. Während das Gesetz eine Information der betroffenen Person nur vorschreibt, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt, sieht die Verordnung vor, dass der Verantwortliche den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mitteilt. Zusätzlich besteht keine gesetzliche Grundlage (Mindestangaben, Dokumentationspflicht) und es entsteht ein Swiss Finish (Angabe von Zeitpunkt und Dauer der Verletzung)

3. Die Dokumentationspflicht gemäss Art. 19 Abs. 5 E-VDSG entbehrt einer gesetzlichen Grundlage und sollte folglich ersatzlos gestrichen werden. Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen Swiss Finish darstellt. Falls an der Dokumentationspflicht festgehalten werden sollte, ist zu präzisieren, dass nur meldepflichtige Verletzungen aufzubewahren sind.
4. «Voraussichtlich» heisst nicht, dass «in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, eine Meldung erfolgen muss» (so die Erläuterungen, S. 32). Der Begriff «voraussichtlich» setzt vielmehr voraus, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko führt. Der Erläuterungsbericht sollte so berichtigt werden, dass in Fällen, wo das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, nicht gemeldet werden muss, sondern nur dann, wenn die Verletzung der Datensicherheit höchstwahrscheinlich zu einem hohen Risiko führt.

Formulierungsvorschlag:
1 Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit:
a. die Art der Verletzung;
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;
e. die Folgen~~, einschliesslich der allfälligen Risiken,~~ für die betroffenen Personen, von welchen ein hohes Risiko ausgeht;
f. gegebenenfalls welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder ~~die Folgen~~ das Risiko zu mildern;
g. den Namen und die Kontaktdaten einer Ansprechperson.
2 Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
3 ~~Der~~ Falls der Verantwortliche verpflichtet ist, die ~~teilt den~~ betroffenen Personen zu informieren, so teilt er ihnen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit.
4 […]
~~5 Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.~~

3. Kapitel: Rechte der betroffenen Person

Artikel 20 (Modalitäten)

Antrag:

1. Die Auskunftserteilung sollte nicht nur schriftlich, sondern auch in einer anderen durch Text nachweisbaren Form möglich sein.
2. Aufnahme der Präzisierung, dass der Begriff «Daten als solche» insbesondere auch eine Auskunft in aggregierter Form zulässt.
3. Ergänzung bzw. Umformulierung von Abs. 3
4. Dokumentationspflicht nach Art. 20 Abs. 5 ist zu streichen.

Begründung:

1. In den Erläuterungen (S. 34) wird festgehalten: «Es kann hier ferner präzisiert werden, dass zur schriftlichen Form auch die elektronische Form gehört.» Diese Präzisierung ist in die Verordnung aufzunehmen.

2. In den Erläuterungen (S. 35) wird ausgeführt: «Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat.» Es besteht im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten bzw. Unterlagen. Vielmehr ist die Mitteilung nach entsprechender Debatte vom Gesetzgeber bewusst beschränkt worden auf die «bearbeiteten Personendaten als solche» (Art. 25 Abs. 2 lit. b revDSG). Damit soll namentlich auch die Auskunft in aggregierter Form ermöglicht werden. Dies sollte zwecks Präzisierung in der Verordnung verankert werden.
3. Betreffend Art. 20 Abs. 3 E-VDSG haben die Mitglieder von economiesuisse zwei verschiedene Vorgehensweisen, um eine Anpassung im Sinne der Wirtschaft vorzunehmen. Einige Mitglieder sprechen sich für eine Streichung des Absatzes aus, während Andere eine Streichung unterstützen würden, aber alternativ für eine Umformulierung plädieren.

   Option 1: Streichung

   Für eine komplette Streichung spricht, dass das Gesetz bereits eine Auskunft an die betroffene Person vorschreibt und auch den Umfang und die Art dieser Auskunft bereits klar und deutlich definiert. 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. Eine weitere Pflicht des Verantwortlichen, einer betroffenen Person diese Auskunft auch noch «verständlich» zu machen, entbehrt einer gesetzlichen Grundlage. Nachdem das Gesetz den Mindestumfang der Auskunft im Detail beschreibt, ist diese zusätzliche Anforderung in der Verordnung auch gar nicht notwendig, dürfte eine Auskunft, welche den gesetzlichen Vorgaben entspricht, regelmässig für jeden Durchschnittsadressaten verständlich sein. Diese Verordnungsbestimmung schiesst zudem über das Ziel hinaus, vgl. Begründung in der Wegleitung: «Werden Personendaten in einer technischen Form geliefert, die für die betroffene Person nicht lesbar und/oder nicht verständlich ist, muss der Verantwortliche imstande sein, ihr ergänzende Erläuterungen zu geben, beispielsweise mündlich.»

   Option 2: Umformulierung

   Art. 20 Abs. 3 E-VDSG verlangt, dass die Auskunft verständlich sein muss. Dies bedeutet nicht, dass der Verantwortliche der um Auskunft ersuchenden Person die Datensätze oder darüber hinaus sogar die damit einhergehenden Abläufe und Geschäftsmodelle erklären muss. Dies könnte im Einzelfall je nach Person mit enormem und unverhältnismässigem Aufwand verbunden sein und wäre je nach Person u.U. gleichwohl untauglich. Zudem könnte eine solche Regelung auch dazu missbraucht werden, das Verfahren und damit den Aufwand für den Verantwortlichen ohne sachlichen Grund «künstlich» zu verlängern.

   Vielmehr muss ausreichend sein, die herauszugebenden Daten so aufzubereiten und darzustellen, dass sie geordnet sind und dadurch unter Anwendung eines objektivierten Masstabes nach Treu und Glauben verständlich sind oder sein müssen. Ob die betroffene Person diese Darstellung im konkreten Fall tatsächlich versteht, kann nicht relevant sein, geht es doch beim datenschutzrechtlichen Auskunftsbegehren nur darum, die bearbeiteten Daten mitzuteilen. Dies entspricht dem Kern des Auskunftsanspruchs, welcher die effektive Herausgabe der relevanten Daten sicherstellt. Darüber hinaus besteht keine Pflicht des Verantwortlichen, die Daten, deren Zweck oder – damit zusammenhängend – die Art der Datenhaltung oder sogar die Geschäftsabläufe zu erläutern. Solches ist schon deshalb abzulehnen, weil dadurch der Aufwand unermesslich und im Einzelfall sogar «never ending» werden könnte. Beispielsweise können die im Rahmen einer klinischen Studie bearbeiteten Daten oder technische Logdaten für die betroffene Person unverständlich sein. Müssen diese zuerst so dargestellt werden, dass sie für die betroffene Person verständlich sind, kann dies oft nicht innerhalb von 30 Tagen erfolgen. Damit würde der Grundsatz der Auskunftserteilung innert 30 Tagen entgegen der gesetzlichen Absicht regelmässig zur Ausnahme.

   Will die auskunftsberechtigte Person mehr über solche über den eigentlichen Herausgabeanspruch hinaus gehende Verhältnisse erfahren, muss sie sich an einen Rechtsanwalt oder Wirtschaftsfachmann halten, nicht an den Verantwortlichen. Demzufolge ist Abs. 3 zusätzlich dahingehend zu klären, dass über die eigentliche «geordnete» Datenherausgabe «keine zusätzlichen Erläuterungen erforderlich» sind.

   Da die Aktivität und die damit einhergehende Verständlichkeit der Auskunft vom Verantwortlichen ausgeht

und von diesem gesteuert werden kann und muss, macht es Sinn, den Verantwortlichen hier bei Abs. 3 mit Bezug auf die Formulierung in den Aktiv-Modus zu setzen.

4. Die Dokumentationspflicht nach Art. 20 Abs. 5 entbehrt einer gesetzlichen Grundlage (vielmehr wurde sie im Rahmen der Vernehmlassung des VE-DSG durch die Pflicht zur Führung eines Verzeichnisses ersetzt). Die DSGVO sieht keine Aufbewahrungspflicht vor, womit diese Regelung einen Swiss Finish darstellt. Die Regelung ist ferner unnötig, da aufgrund der Beweislast ohnehin im Interesse des Verantwortlichen, mit Dokumentation den Nachweis erbringen zu können.

Formulierungsvorschlag
1-2 […]
3 ~~Die Auskunft muss für die betroffene Person verständlich sein.~~ Der Verantwortliche muss die Auskunft geordnet vornehmen. Zusätzliche Erläuterungen sind nicht erforderlich.
Oder
~~3 Die Auskunft muss für die betroffene Person verständlich sein.~~
4 Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.
~~5 Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.~~

Artikel 21 (Zuständigkeit)

Antrag:

1. Streichung Abs. 1 Satz 2
2. Konkretisierung Abs. 2

Begründung:

1. Der erste Satz von Art. 21 Abs. 1 E-VDSG ist nicht zu beanstanden. Der zweite Satz stellt demgegenüber eine Forderung auf, welche im operativen Alltag regelmässig gar nicht erfüllt werden kann. In manchen Konstellationen ist für einen Verantwortlichen weder klar noch eindeutig ersichtlich, inwieweit für einen bestimmten Sachverhalt ein anderer Verantwortlicher zuständig sein soll und wer dies gegebenenfalls ist. In vielen Fällen kann ein Verantwortlicher deshalb der Pflicht, das Begehren an den zuständigen Verantwortlichen weiterzuleiten, naturgemäss gar nicht nachkommen. In unklaren Fällen ein Auskunftsbegehren an andere, vermeintlich zuständige Verantwortliche, weiterzuleiten, würde dem Datenschutz geradezu entgegenlaufen, erhielten doch auf diese Weise womöglich Personen Kenntnis vom Fall, welche gar nicht als Verantwortliche qualifiziert wurden. Einer fälschlicherweise um Auskunft ersuchten Person ist es auch nicht zuzumuten, abzuklären, wer an seiner Stelle Verantwortlicher sein könnte. Auch solche Abklärungen würden dem berechtigten Bedürfnis der um Auskunft ersuchenden Person nach Einhaltung des Datenschutzes gerade zuwiderlaufen.
2. Auftragsbearbeiter sind nicht darauf eingerichtet, Auskunft zu erteilen, weil sie keine entsprechende gesetzliche oder vertragliche Pflicht haben. Der Verweis auf eine Auskunftserteilung durch den Auftragsbearbeiter ist deshalb falsch und kann in der Praxis Probleme schaffen. Gemeint ist hier wohl vielmehr, dass Auftragsbearbeiter den Verantwortlichen bei der Auskunftserteilung unterstützen sollen, was in der Praxis ohnehin jeweils so vereinbart wird.
   Des Weiteren ist Art. 21 Abs. 2 E-VDSG verwirrlich, da er impliziert, dass der Auftragsbearbeiter selbst eine Auskunftspflicht hat, wenn er faktisch in der Lage sein sollte, eine Auskunft zu erteilen bzw. er das Auskunftsgesuch in einem solchen Fall nicht weiterleiten muss, auch wenn er es nicht beantwortet. Das kann

nicht sein. Im Gegenteil ist es dem Auftragsbearbeiter i.d.R. vertraglich untersagt, selbst Auskunft zu erteilen, wenn ein Auskunftsbegehren direkt bei ihnen eingehen sollte. Der letzte Halbsatz von Abs. « («sofern er nicht in der Lage ist, selbst Auskunft zu geben») ist zu streichen und durch die Formulierung "sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet» zu ersetzen.

Formulierungsvorschlag:
1. Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~
2. Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so ~~leitet der Verantwortliche das Begehren zur Erledigung an den Auftragsbearbeiter weiter,~~ unterstützt der Auftragsbearbeiter den Verantwortlichen bei der Erteilung der Auskunft, sofern er ~~nicht in der Lage ist, selbst Auskunft zu erteilen~~ das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.

Artikel 22 (Frist)

Antrag:
Der Fristbeginn ist zu präzisieren.

Begründung:
Wenn aus dem Auskunftsbegehren nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, soll die Frist erst mit dieser Klarstellung zu laufen beginnen. Zudem ist klarzustellen, dass erst der Eingang des Begehrens beim Verantwortlichen fristauslösend ist und nicht etwa beim Auftragsbearbeiter, falls ein Betroffener das Begehren dem Auftragsbearbeiter zugestellt und dieser das Begehren dem Verantwortlichen weiterleitet.

Formulierungsvorschlag:
1 Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens beim Verantwortlichen erteilt. Erfordert das Begehren einer Präzisierung, welche Daten die betroffene Person wünscht, beginnt die Frist mit Zugang der Präzisierung beim Verantwortlichen zu laufen. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.

Artikel 23 (Ausnahme von der Kostenlosigkeit)

Antrag:

1. Der Maximalbetrag von CHF 300.- ist zu streichen.
2. Der Fristbeginn sollte ergänzt werden, um die 30 Tage sicherzustellen.

Begründung:

1. Der Maximalbetrag von CHF 300.-- wird den tatsächlichen Verhältnissen und dem damit verbundenen Aufwand nicht ansatzweise gerecht. Sind z.B. zur Sicherstellung des Datenschutzes von Dritten umfangreiche Schwärzungen notwendig, kann dies im Einzelfall durchaus höhere Aufwendungen mit sich bringen. Art. 23 Abs. 2 E-VDSG sollte deshalb gestrichen werden, da die die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist und keine weiteren Einschränkungen nötig sind.
2. Abs. 3 muss dahingehend angepasst werden, dass die in Abs. 1 geregelte Frist von 30 Tagen zur Auskunftserteilung nicht faktisch auf 20 Tage abgekürzt werden kann. Dies kann durch eine Ergänzung des Fristbeginns in Abs. 3 sichergestellt werden.

Formulierungsvorschlag:
1 Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden~~,~~ oder querulatorisch ist.
~~2 Die Beteiligung beträgt maximal 300Franken.~~
3 Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen. Die Frist zur Auskunftserteilung beginnt mit Ablauf der Rückzugsfrist.

4. Kapitel: Rechte der betroffenen Person

Artikel 25 (Datenschutzberaterin und Datenschutzberater)

Antrag:

1. Art. 25 Abs. 1 lit. b E-VDSG ist ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 lit. a E-VDSG direkt in Abs. 1 integriert werden.
2. Das Interventionsrecht gemäss lit. b ist zur Vervollständigung einer konzeptionell in sich stimmigen «Good Governance» mit dem Eskalationsrecht in einer neuen lit. c zu ergänzen.

Begründung:

1. Die gesetzliche Regelung zur Funktion der Datenschutzberatung wird auf Verordnungsstufe eingeengt.
   Die Datenschutzberaterin oder der Datenschutzberater muss lediglich beratend Einfluss nehmen, damit der Verantwortliche die Datenschutzpflichten richtig anwendet (vgl. Art. 10 revDSG, insb. Abs. 2 lit. b). Bei der Formulierung von Art. 25 Abs. 1 lit. a E-VDSG bleibt mit der Formulierung «prüft» der Umfang der Prüfpflicht unklar. Die Funktion Datenschutzberatung kann jedenfalls nicht jede beim Verantwortlichen anfallende Datenbearbeitung prüfen. Der Verantwortliche kann aber in Absprache mit der Funktion Datenschutzberatung eine interne Governance schaffen, welche in geeigneter Form die internen Regeln zu diesem Thema festlegt. So sollte die Funktion Datenschutzberatung nur solche Datenbearbeitungen prüfen, welche ihr effektiv vorgelegt werden. Dies auch zum eigenen Schutz. Ausserhalb der Konsultationspflicht muss die Funktion Datenschutzberatung entsprechend ihrer Hauptfunktion nur allgemein beratend tätig sein. Zur Klarstellung dieser Verhältnisse ist – auch zum Schutz von Datenschutzberatenden, für welche keine spezifische interne Governance besteht – die in Art. 25 Abs. 1 Bst a genannte Prüfpflicht auf «ihm vorgelegte» Datenbearbeitungen einzugrenzen.
   Die Regelung von Art. 25 Abs. 1 Bst b E-VDSG widerspricht der Funktion Datenschutzberatung und überdies der Organisationsfreiheit des Verantwortlichen, wie genau die Pflichten gemäss revDSG unter Würdigung der konkreten Verhältnisse im Unternehmen personell, technisch und organisatorisch am besten erfüllt werden sollen. Insofern liegt ein nicht stufengerechter Eingriff in die Privatautonomie des Unternehmens vor.
   Ferner verletzt die Bestimmung das weltweit als Standard etablierte drei Linien Verteidigungsmodell, in dem es die Erkennung, Einhaltung und Korrektur von datenschutzrechtlichen Vorgaben einer einzelnen Funktion, namentlich der Datenschutzberaterin oder dem Datenschutzberater, auferlegt.
   Schliesslich macht die vorgeschlagene Regelung von Art. 25 Abs. 1 lit. b E-VDSG die übergeordnete Ausnahmeregelung von Art. 23 Abs. 4 revDSG obsolet oder anders gesagt: Art. 25 Abs. 1 lit. b E-VDSG ist gar nicht nötig, weil mit Art. 23 Abs. 4 revDSG bereits eine ausreichende, übergeordnete Regelung besteht.

   Nach alledem ist Art. 25 Abs. 1 lit. b E-VDSG ersatzlos zu streichen. Dementsprechend kann Art. 25 Abs. 1 lit. a E-VDSG direkt in Abs. 1 integriert werden, was die Regelung etwas kürzer macht (siehe folgender Formulierungsvorschlag).

2. Art. 25 Abs. 2 lit. b E-VDSG regelt zu Recht ein Interventionsrecht. Dies ist nötig, damit die oder der Datenschutzberater/in bei unternehmensinternen Prüfungen der Einhaltung datenschutzrechtlicher Regeln nicht nur den Worten bzw. den ihm zur Verfügung gestellten Dokumenten vertrauen muss, sondern – soweit sinnvoll und nötig – die Beschaffung zusätzlicher Informationen und Dokumente durchsetzen kann. Mit dieser Regelung bleibt Art. 25 Abs. 2 lit. b E-VDSG aber «auf halbem Weg» stehen. Stösst die Datenschutzberaterin oder der Datenschutzberater nämlich bei der Ausübung des Interventionsrechts auf Unstimmigkeiten und sind die Linienverantwortlichen nicht gewillt, entsprechend dem Ratschlag der Datenschutzberaterin oder des Datenschutzberaters Abhilfe zu schaffen, muss Letzterer oder Letzterem spiegelbildlich zum Interventionsrecht bzw. zur Vervollständigung des Gesamtprozesses überdies ein Eskalationsrecht zustehen. Ein solches Recht ist sachlogisch keine Pflicht. Die Datenschutzberaterin oder der Datenschutzberater erhält damit aber das notwendige Instrumentarium, zumindest im Fall komplexer Verhältnisse und besonders schwerwiegende Verstösse gegen Datenschutzpflichten notfalls, mithin als Ausnahme von der Regel, die Thematik im Rahmen und allenfalls in Absprache mit der Compliance-Organisation, soweit eine solche besteht, auf dem Linienweg nach oben zu eskalieren und auf diese Weise auf höherer Stufe zum Entscheid zu bringen bzw. bringen zu lassen, nötigenfalls bis zum höchsten Organ des Unternehmens, und damit klare Verhältnisse zu schaffen. Bei einfacheren Strukturen genügt es aber auch, wenn die Funktion Datenschutzberatung in wichtigen Fällen die höchsten Organe lediglich informiert. Andernfalls setzt sich die Datenschutzberaterin oder der Datenschutzberater gerade bei schwerwiegenden Verstössen gegen Datenschutzpflichten dem Risiko aus, mangels Eskalationsmöglichkeit im Schadensfall selbst haftbar zu werden, weil ihr oder ihm vorgeworfen wird, sich nicht hartnäckig genug eingesetzt zu haben. Art. 25 Abs. 2 ist somit mit einer lit. c zu ergänzen, welche ergänzend zum Interventionsrecht nach lit. b das Eskalationsrecht regelt.

Formulierungsvorschlag:
1 Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen ~~muss folgende Aufgaben wahrnehmen: a. Sie oder er~~ prüft die ihr oder ihm vorgelegten Bearbeitungen von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass rechtliche Datenschutzvorschriften verletzt wurden.
~~b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.~~
2 Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater:
a. die notwendigen Ressourcen zur Verfügung stellen;
b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.
c. das Recht einräumen, in wichtigen Fällen die höchsten Organe zu informieren.

Artikel 26 (Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten)

Antrag:
Es ist zu präzisieren, dass sich die allfällige Pflicht eines KMU zur Führung eines Verzeichnisses nicht auf sämtliche Bearbeitungen erstreckt, sondern auf diejenigen Bearbeitungen beschränkt ist, welche die Voraussetzung(en) triggern.

Begründung:
Der Bundesrat hat gemäss Art. 12 Abs. 5 revDSG Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses vorzusehen für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und deren Datenbearbeitung ein «geringes Risiko» mit sich bringt. Gemäss E-VDSG 26 bedeutet ein geringes Risiko, dass weder «umfangreich besonders schützenswerte Personendaten bearbeite» werden, noch «ein Profiling mit hohem Risiko durchgeführt» wird. Alle anderen Bearbeitungen bringen im Umkehrschluss ein geringes Risiko mit sich.

Durch Präzisierung, dass sich die Pflicht zur Führung eines Verzeichnisses ausschliesslich auf diejenigen Bearbeitungen erstreckt, welche die Voraussetzung triggern, kann sowohl dem Schutz der betroffenen Personen als auch den Bedürfnissen der KMU angemessen Rechnung getragen werden (vgl. auch das Positionspapier des EDSA zu Art. 30 Abs. 5 DSGVO).

Es ist ferner zu präzisieren, dass das Verzeichnis nicht schriftlich, sondern auch in anderer Form, die den Nachweis durch Text ermöglicht, z.B. elektronisch, geführt werden kann. Damit ist klargestellt, dass das Verzeichnis auch elektronisch geführt werden kann.

Formulierungsvorschlag:
1 Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:
a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet.
b. Es wird ein Profiling mit hohem Risiko durchgeführt.
2 Ist eine Voraussetzung nach Abs. 1 lit. a und/oder b erfüllt, so ist die Verzeichnispflicht auf diejenige Bearbeitung bzw. diejenigen Bearbeitungen beschränkt, welche dieser Voraussetzung bzw. diesen Voraussetzungen zugrunde liegen.
3 Das Bearbeitungsverzeichnis ist schriftlich, oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu führen.

7. Kapitel: Schlussbestimmungen

Antrag:
Das lückenhafte Übergangsregime auf Stufe des revDSG ist auf Verordnungsstufe mit zusätzlichen Übergangsbestimmungen zu ergänzen.

Begründung:
Für sämtliche neuen Pflichten, welche erheblichen Aufwand generieren, müssen angemessene Übergangfristen bestehen, zumal IT-gestützte Lösungen nötig sind.

Dabei ist zu berücksichtigen, dass die verschiedenen Regeln und Pflichten des gesamten Regelwerks (Gesetz samt Verordnung) gegenseitige Wechselwirkungen generieren. Die neuen Regeln bzw. Pflichten sind deshalb zusammen mit den unverändert weiter geltenden Regeln bzw. Pflichten zu einem in sich stimmigen Gesamtkonzept zu verschmelzen. Ein solches Gesamtkonzept kann sachlogisch erst nach Vorliegen der finalen Texte auf Gesetzes- und Verordnungsstufe erarbeitet, final festgelegt und umfassend in die IT-Sprache «übersetzt» werden. Erst danach kann mit dem Aufbau der IT-gestützten Lösung begonnen werden. Vor der «Go live»-Schaltung sind sodann die nach bewährten Standards vorgesehenen Tests durchzuführen. Parallel dazu sind auch die Mitarbeitenden entsprechend ihrer jeweiligen Funktion auszubilden und überdies die Verträge mit Lieferanten und Geschäftspartnern anzupassen.

Für alle diese notwendigen Aktivitäten ist gemäss etablierten Erfahrungswerten ein Zeitraum von rund 2 Jahren ab Vorliegen der finalen Gesetzes- und Verordnungstexte notwendig. Im Gegenzug stellt eine solche IT-gestützte Lösung die gleichförmige Anwendung sämtlicher Regeln innerhalb des gesamten Unternehmens sicher.

Aus den genannten Gründen hat die EU seinerzeit entschieden, für die Umsetzung der EU-DSGVO nicht Übergangsfristen für einzelne Regeln bzw. Pflichten, sondern pauschal 2 Jahre für das gesamte Regelwerk zuzugestehen.

In der Schweiz hat das Parlament für das revDSG eine andere Grundentscheidung getroffen (vgl. Art. 68-74 revDSG). Im Rahmen des parlamentarischen Prozesses liegt der Fokus naturgemäss auf den materiellen Regeln bzw. Pflichten. Das kam beim revDSG besonders deutlich zum Ausdruck, wurde doch über den konkreten Wortlaut einiger zentraler Bestimmungen wie z.B. zum Profiling (Art. 5 lit. f und g revDSG) buchstäblich bis zum Schluss heftig debattiert. Die Übergangsbestimmungen kommen deshalb im parlamentarischen Prozess regelmässig zu kurz, was beim revDSG in erhöhtem Mass der Fall war. Übergangsbestimmungen sollen zudem strikt nach sachlichen Kriterien festgelegt werden und nicht «Spielball» politischer Kompromisse sein. Deshalb hat es sich im schweizerischen Gesetzgebungsprozess inzwischen eingebürgert, falls notwendig ergänzende Übergansbestimmungen auf Verordnungsstufe festzulegen.

Im Zuge der DSG-Revision ist zumindest für folgende entweder neu eingeführten oder zumindest mit neuen Anforderungen konfrontierten Regeln bzw. Pflichten mit offensichtlich erheblichem Umsetzungsbedarf auf Gesetzesstufe keine Übergangsbestimmung festgelegt worden:

- Pflicht, eine angemessene Datensicherheit zu gewährleisten (Art. 8 revDSG i.V.m. Art. 1ff. E-VDSG);
- Pflicht zur Erstellung des Verzeichnisses der Datenbearbeitungstätigkeiten (Art. 12 revDSG);
- Pflicht, so rasch als möglich Meldung von Verletzungen der Datensicherheit zu erstatten (Art. 24 revDSG i.V.m. Art. 19 E-VDSG).

Gerade diese drei zentralen Pflichten können naturgemäss erst gestützt auf das Vorliegen eines umfassenden, in sich stimmigen Gesamtkonzepts sämtlicher Regeln bzw. Pflichten zielführend und final festgelegt werden.

Der finale Wortlaut der E-VDSG wird wohl erst gegen Ende des Jahres 2021 vorliegen. Unter Mitberücksichtigung des Umstandes, dass gestützt auf den Wortlaut des revDSG mit den Umsetzungsarbeiten zumindest schon begonnen werden konnte, ist nach dem Gesagten für die beiden vorgenannten Pflichten eine Übergangsfrist bis allermindestens 1. Juli 2023 notwendig, wobei die Aufrechterhaltung der Äquivalenz sichergestellt werden muss.

Formulierungsvorschlag:
Art. 48 ~~Inkrafttreten~~ Übergangsbestimmung betreffend das Verzeichnis der Bearbeitungstätigkeiten und der Meldung von Verletzungen der Datensicherheit
~~Diese Verordnung tritt am ... in Kraft~~. Art. 12 und 24 des Gesetzes sind erst ab 1. Januar 2023 zu erfüllen.

In der Folge würde Art. 48 E-VDSG (Inkrafttreten) neu zu Art. 49 E-VDSG.

Art. 48~~49~~ Inkrafttreten
Diese Verordnung tritt am ... in Kraft.

Eventualiter:
Alternativ zum neuen Art. 48 E-VDSG kann stattdessen das Inkrafttreten des ganzen Gesetzgebungspakets (revDSG und E-VDSG) nach hinten auf den 1. Juli 2023 geschoben werden (dynamisches Verhältnis zwischen Inkrafttreten und Übergangsfristen).

Da zwischen dem Abschluss des revDSG und der Vernehmlassung zur VDSG fast ein Jahr verstrichen ist, sollte die Dringlichkeit nicht mehr als Hauptargument einer raschen Inkraftsetzung genannt werden. Zudem brauchen die Unternehmen für die Umsetzung der Verordnung auch ausreichend Zeit. Dies vor allem auf Grund der zusätzlichen Anforderungen, welche durch die VDSG entstehen.