Swico
Lagerstrasse 33
CH-8004 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

Frau Bundesrätin Karin Keller-Sutter
Eidgenössiches Justiz- und Polizeidepartement EJPD

Ausschliesslich per Mail an:
Jonas.amstutz@bj.admin.ch

Zürich, 14. Oktober 2021

**Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG); Vernehmlassungsantwort**

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese gerne innerhalb der angesetzten Frist wahr.

Swico ist der Wirtschaftsverband der Digitalisierer und vertritt die Interessen etablierter Unternehmen sowie auch Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 650 Mitglieder aus der ICT- und Online-Branche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken. Neben Interessenvertretung betreibt Swico das nationale Rücknahmesystem «Swico Recycling» für Elektronik-Altgeräte.

Für unsere Branche ist ein modernisierter Datenschutz zentral, der Innovation nicht übermässig einschränkt, administrativ tragbar ist und angemessen im Rahmen der internationalen Entwicklungen ausfällt. Die vorliegende Verordnungslösung weist jedoch mehrfache Unstimmigkeiten auf, die es ohne Gefährdung des Zeitplans hinsichtlich der Äquivalenzanerkennung durch die Europäische Union zu bereinigen gilt. Insbesondere ist auf einen Swiss Finish zu verzichten und der Wille des Gesetzgebers zu respektieren.

## 1. Grundsätzliche Bemerkungen

Das neue Datenschutzgesetz (revDSG) war Gegenstand langer parlamentarischer Diskussionen, an denen unterschiedliche Lager beteiligt waren. Die Wirtschaft hat sich stets für eine administrativ tragbare, gegenüber der EU angemessene Lösung ohne Swiss Finish eingesetzt. Das Ergebnis der Beratungen war eine Kompromisslösung. Der vorliegende Entwurf trägt diesem Kompromiss ungenügend Rechnung. An einzelnen Stellen sind sogar Bestimmungen eingeflossen, welche im Verlauf des Gesetzgebungsprozesses zum revDSG bewusst gestrichen wurden und entsprechend nicht Teil des Schlussabstimmungstextes sind.

Die Bereinigung des vorliegenden E-VDSG sollte so erfolgen, dass der Zeitplan hinsichtlich des Äquivalenzbeschlusses der EU gegenüber der Schweiz nicht gefährdet wird, denn unsere Mitglieder sind in einem besonderen Masse auf einen barrierefreien Datenaustausch mit der EU angewiesen

Unseres Erachtens ist der E-VDSG mit Mängeln durchzogen, welche unter folgenden Oberbegriffen zusammengefasst werden können (detaillierte Erklärungen hierzu sind jeweils unter den Kommentaren zu den einzelnen Bestimmungen angebracht):

- **Swiss Finish muss auch in der VDSG beseitigt werden**: Schweizer Besonderheiten, welche über die europäische Regulierung hinausgehen, schaffen für die Schweizer ICT-Branche sowie für die Gesamtwirtschaft erheblichen administrativen Mehraufwand ohne effektiven Nutzen für Konsumentinnen und Konsumenten. Entsprechend wurde in der Diskussion zum Gesetzgebungsprozess zum revDSG darauf geachtet, derartige Regelungen weitgehend zu vermeide bzw. zu beseitigen. Dies muss auch für die VDSG gelten. Es ist nicht ersichtlich, auf welcher Grundlage der E-VDSG zahlreiche Swiss Finish enthält.
- **Verordnungsbestimmungen ohne hinreichende gesetzliche Grundlage im revDSG:** Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detail-vorschriften näher auszuführen, um zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt hingegen eine entsprechende Delegationsnorm im Gesetz voraus. Vorliegend enthält der E-VDSG viele Bestimmungen, die im Gesetz hätten geregelt werden müssen und nicht auf dem Verordnungswege eingeführt werden können.

- **Politischer Prozess zum revDSG wurde nicht respektiert:** Der E-VDSG versucht Bestimmungen einzuführen, auf die im langwierigen politischen Prozess im Sinne einer Kompromisslösung verzichtet wurde. Zudem enthält er statt notwendiger Klarstellungen praxisfremde Regelungen oder führt parallele Verzeichnispflichten und sonstigen neuen Administrativaufwand ein – ohne erkenntlichen Nutzen. Leider trägt auch der erläuternde Bericht hier nicht zur Klärung bei.

## 2. Detaillierte Streichungs- und Anpassungsvorschläge

- Art. 2 Schutzziele (Datensicherheit): *Anpassen*.

Mit diesem Artikel wird die bereits bekannte Liste von Schutzzielen erweitert in Bezug auf die Massnahmen zur Gewährleistung der Datensicherheit. Die Liste fällt zu absolut aus: Mit der gewählten Formulierung wird der Eindruck erweckt, dass es sich um absolut zu erreichende Anforderungen handelt. Zu treffen sind angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich. Entsprechend ist der Wortlaut zu ändern und «erreichen» mit «anstreben» zu ersetzen.

Zudem enthält die Bestimmung zu detaillierte Formulierungen. Im Kern muss es im hier zu regelnden Bereich der Datensicherheit um die klassischen Schutzziele Integrität, Verfügbarkeit und Belastbarkeit gehen. Eine generelle Dokumentationspflicht wurde vom Gesetzgeber verworfen. Die Reduktion von lit. a bis lit. k auf die genannten Begriffe stimmt zudem mit Art. 32 DSGVO überein. Andernfalls liegt ein Swiss Finish vor.

- Art. 3 Abs. 1 bis 4 E-VDSG Protokollierung (Datensicherheit): *Streichen*.

Ergibt eine Datenschutz-Folgenabschätzung (DSFA) ein «hohes Risiko», so wird für die Datenbearbeitung mit dieser Norm ein Audit-Trail vorgesehen (Protokollieren von Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten). Die Audit-Trails sind gemäss Verordnungstext für zwei Jahre aufzubewahren (in vom operativen System getrennten Systemen) und die Protokolle dürfen nur für Datenschutzzwecke aufbewahrt werden.

Wir beantragen, diese Norm ersatzlos zu streichen, da sie mit einem massiven Datenbearbeitungsaufwand und schwieriger technischer Umsetzbarkeit einhergeht. Beispielsweise ist nicht klar, wie die Protokollierung des Elements «Lesen» in der Praxis erfolgen soll.

Die Pflicht zur Protokollierung nach Abs. 1 stammt aus der geltenden VDSG und sollte die Nachvollziehbarkeit einer Datenbearbeitung sicherstellen, wenn der Datenschutz nicht eingehalten werden konnte. Diese Ausgangslage gibt es bei der DSFA nicht: Dort muss bei einer Bearbeitung mit hohem Risiko der EDÖB konsultiert werden. Die Protokollierung entfällt dabei, da der Datenschutz in diesem Fall eingehalten wurde. Die Regelung stellt einen Swiss Finish dar und es fehlt die gesetzliche Grundlage dazu. Unklar und offen lässt der neue Verordnungstext, ob die Verletzung der Protokollierungspflicht gegebenenfalls auch eine strafbare Verletzung der Datensicherheit darstellen kann.

Sollte dennoch an dieser Bestimmung festgehalten werden, so müsste auf alle Fälle die Frist für die Pflicht zur Vorhaltung von Sicherheits-Logs auf einem Jahr belassen und nicht neu auf zwei Jahre ausgeweitet werden (Art. 3 Abs. 4 E-VDSG). Eine zweijährige Frist geht über die anerkannte Security Praxis hinaus (z.B. internationale Standards wie NIST 800-92), in der 12 Monate Standard sind für die Vorhaltung von Sicherheitsprotokollen aus Systemen, aus denen ein «hohes Risiko» für die Bearbeitung der personenbezogenen Daten hervorgeht. Durch eine zweijährige Frist würden die Kosten des oben genannten massiven Datenbearbeitungs-volumens unverhältnismässig verdoppelt. Es ist zu betonen, dass Protokollierungen insbesondere zur raschen Aufdeckung von Sicherheitsverletzungen dienen und nur in Zusammenhang mit einem Intrusion Detection and Prevention System (IDPS) Sinn machen, was zwar in den TOMs unter Art. 2 E-VDSG angesprochen wird, jedoch nicht in den Kontext der Protokollierung gesetzt wird.

- Art. 4 Abs. 1 bis 3 E-VDSG Bearbeitungsreglement von privaten Personen (Daten-sicherheit): *Streichen*.

Diese Bestimmung sieht die Pflicht zur Führung eines Bearbeitungsreglements vor, wenn besonders schützenswerte Personendaten umfangreich bearbeitet werden oder bei einem Profiling mit hohem Risiko. Für dieses Bearbeitungsreglement werden Mindestangaben vorgesehen (z.B. Angaben zu den Massnahmen, die zur Datenminimierung getroffen wurden).

Wir beantragen diesen Artikel zur Streichung, da er einen unnötigen administrativen Mehraufwand in Form eines separaten Zusatzdokuments fordert, das der Verantwortliche unterhalten muss. Die Norm verwischt die Grenzen zwischen etablierten Instrumenten wie DSFA, Bearbeitungsverzeichnis, Datenschutztraining und internen Richtlinien und ist unnötig. Diese haben sich in der Praxis als effektive Mittel bewährt. Die Bestimmung schafft insbesondere eine unnötige Doppelspurigkeit zum Verzeichnis der Bearbeitungstätigkeiten nach Art. 12 revDSG. Im erläuternden Bericht ist nicht ersichtlich, worin der Mehrwert des neuen Bearbeitungsreglements gesehen wird. Auf eine Bestimmung dieser Art wurde zudem im Laufe des Vernehmlassungsprozesses bewusst verzichtet, was zu respektieren ist. Auch hier ist eine fehlende Rechtsgrundlage im revDSG festzustellen: Art. 8 revDSG regelt nur die Datensicherheit i.e.S. und nicht die Einhaltung der Bearbeitungsgrundsätze, worauf Art. 4 E-VDSG abzielt. Bereits für die Vorgängernorm in der aktuellen VDSG fehlte eine gesetzliche Grundlage, weshalb sie toter Buchstabe blieb. Zudem handelt es sich beim Inhalt dieser Bestimmung erneut um einen Swiss Finish.

Sollte an der Bestimmung dennoch festgehalten werden, so ist es zentral, den Anwendungsbereich auf den Verantwortlichen einzuschränken und nicht auch auf den Auftragsbearbeiter auszuweiten (Abs. 1). Dies ist auch unter bisherigem Recht der Fall («Inhaber der Datensammlung» gem. Art. 11 VDSG) und notwendig, um die Grenzen der Rechenschaft zwischen dem Verantwortlichen und dem Auftragsbearbeiter nicht zu verwässern.

- Art. 5 Abs. 1 bis 3 E-VDSG: Bearbeitungsreglement von Bundesorganen: *Streichen.*

Art. 5 E-VDSG hält fest, dass Bundesorgane und deren Auftragsbearbeiter in den Fällen von Abs. 1 lit. a bis f für sämtliche automatisierten Datenbearbeitungen ein Bearbeitungsreglement erstellen müssen. Für das Bearbeitungsreglement werden dieselben Mindestangaben wie bei den Privaten vorgesehen.

Wir beantragen die Streichung des Artikels aus den gleichen Gründen, die bereits bei Art. 4 E-VDSG für Private aufgeführt wurden: Der Anwendungsbereich würde für Bundesorgane praktisch für jede automatisierte Bearbeitung gelten. Zu einem Zusatznutzen führt die Bestimmung auch bei Bundesorganen nicht, da die bereits etablierten Dokumentationspflichten wie die DSFA oder Bearbeitungsverzeichnisse auch für Bundesorgane gelten. Analog den Ausführungen zu Art. 4 E-VDSG fehlt es auch dieser Bestimmung an der gesetzlichen Grundlage.

- Art. 6 E-VDSG Modalitäten der Bearbeitung durch den Auftragsbearbeiter. *Streichen Abs. 1 und 2, Klarstellen Abs. 3.*

Art. 6 Abs. 1 E-VDSG hält fest, dass der Verantwortliche, welcher die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, für den Datenschutz verantwortlich bleibt. Dabei muss er sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

Für den Verantwortlichen ist es in der Praxis nicht möglich, das Kriterium der «Sicherstellung» betreffend die vertrags- und gesetzesgemässe Bearbeitung zu erfüllen. Er kann höchstens dazu «Sorge tragen». Diese Unterscheidung ist wesentlich, da der Verantwortliche datenschutzrechtlich haftbar bleibt, zivilrechtlich jedoch nur bei Verschulden (Art. 41 ff. OR) und nicht etwa kausal. Die vorliegende Einrichtung einer Kausalhaftung ist nicht nötig, da die allgemeinen Haftungsregeln nach OR greifen. Auch hier fehlt unseres Erachtens eine Rechtsgrundlage im revDSG und wir sehen hier erneut einen Swiss Finish.

Art. 6 Abs. 2 E-VDSG hält weiter fest, dass – im Falle des Nichtunterliegens des Auftragsdatenbearbeiters unter das DSG – der Verantwortliche sich bei einem Auslandtransfer vergewissern muss, dass andere gesetzliche Datenschutzbestimmungen mit demselben Niveau greifen oder dieses vertraglich sicherstellen. Wir beantragen auch diesen Absatz zur Streichung, da keine Notwendigkeit besteht: Auslandtransfers sind abschliessend in Abschnitt 3 revDSG geregelt. Zudem regelt Abs. 2 den Gegenstand des Auslandtransfers nur ungenügend bzw. nicht abschliessend.

Art. 6 Abs. 3 E-VDSG hält schliesslich für Bundesorgane fest, dass der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen darf, wenn das Bundesorgan als Verantwortlicher dies schriftlich genehmigt hat. Diesbezüglich ist explizit klarzustellen, dass eine Genehmigung auch in elektronischer Textform genügt und sie in allgemeiner Form erfolgen kann (analog der DSGVO). Die Ausführungen in der Botschaft zu Art. 6 Abs. 3 E-VDSG lassen dies klar zu. Dienste von Standard-Online-Providern, welche durch Bundesorgane bezogen werden, sehen ausschliesslich diese Methode vor.

- Art 7 E-VDSG Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans: *Streichen oder anpassen.*

Nach Art. 7 E-VDSG müssten Datenschutzberaterinnen oder -Berater von Bundesorganen den EDÖB umgehend informieren über den Abschluss von Auftragsdatenbearbeitung, die Genehmigung der Übertragung von Datenbearbeitungen an Dritte oder über allgemeine Probleme bei der Einhaltung von Datenschutzvorschriften. Mit Art. 29 E-VDSG besteht bereits eine Informationspflicht, welche allgemeiner formuliert ist und auch die Auftragsbearbeitungen umfasst, sofern diese relevant sind. Welche «Probleme» zu melden sind, ist zudem unklar. Deshalb beantragen wir die Streichung oder eventualiter die entsprechende Anpassung der Bestimmung.

- Art. 8 E-VDSG Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs (Bekanntgabe von Personendaten ins Ausland): *Anpassen*.

Der Bundesrat legt nach Art. 16 Abs. 1 revDSG fest, welche Staaten oder internationalen Organisationen einen angemessenen Datenschutz gewährleisten. Die vorliegende Bestimmung kann jedoch in einer Art missverstanden werden, dass die verantwortliche Stelle und nicht der Bundesrat die Angemessenheit des Datenschutzes im Empfängerstaat feststellen muss. In Art. 8 E-VDSG ist deshalb klar zum Ausdruck zu bringen, dass sich diese Bestimmung ausschliesslich an den Bundesrat richtet.

- Art. 9 E-VDSG Datenschutzklauseln und spezifische Garantien (Bekanntgabe von Personendaten ins Ausland): *Streichen Abs. 1 und Abs. 2.*

Diese Bestimmung legt inhaltliche Vorgaben für Datenschutzklauseln zum Schutz von Personendaten in unsicheren Drittländern fest (z.B. Einhaltung der Bearbeitungsgrundsätze, Namen der Empfängerstaaten, Anforderungen an die Aufbewahrung und Löschung von Daten).

Der Anwendungsbereich dieser Bestimmung bezieht sich auf die Standardvertragsklauseln der EU-Kommission (SCC), welche in der Praxis überwiegend verwendet werden. Abs. 1 sollte entsprechend keine Vorgaben machen, die mit den SCC nicht konform sind. Die DSGVO leistet einen angemessenen Schutz. Dieser ist für Datenbekanntgaben durch Schweizer Verantwortliche ebenso gut. Deshalb ist der Abs. 1 unseres Erachtens überflüssig.

Abs. 2 sieht die Pflicht des Verantwortlichen vor, sicherzustellen, dass der Empfänger im Ausland diese Datenschutzklauseln auch einhält. Diese Bestimmung ist ersatzlos zu streichen: Abs. 2 ist zu unbestimmt, da nicht hervorgeht, was diese Massnahmen sein könnten. Neben der unrealistischen Regelungsabsicht fehlt es an einer gesetzlichen Grundlage, und auch die DSGVO kennt keine solche Regelung.

- Art. 10 Abs. 1 E-VDSG Standardschutzklauseln (Bekanntgabe von Personendaten ins Ausland): *Streichen.*

Abs. 1 dieser Bestimmung (der Exporteur trifft angemessene Massahmen, um sicherzustellen, dass der Importeur die Klauseln beachtet) ist durch die neuen SCC eigentlich überflüssig geworden. Sie ist zudem zu unbestimmt und es ist nicht klar, was diese Massnahmen sein könnten. Der Exporteur kann in der Praxis nicht sicherstellen, dass der Empfänger die Klauseln beachtet. Er kann es nur verlangen und im Rahmen der neuen SCC (Klausel 14) prüfen, ob lokales Recht der Einhaltung entgegensteht. Dieser Verordnungsbestimmung fehlt es zudem ebenso an der gesetzlichen Grundlage.

- Überschrift «2. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters»: *Kürzen.*

Den Auftragsbearbeiter treffen keine gesetzlichen Informationspflichten, weshalb dieser aus der genannten Überschrift zu streichen ist.

- Art. 13 E-VDSG Modalitäten der Informationspflichten (Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters): *Streichen des Auftragsdatenbearbeiters in Abs. 1 und Streichen von Abs. 2.*

Diese Bestimmung hält in Abs. 1 eine Informationspflicht für den Auftragsdatenbearbeiter fest. Dieser ist jedoch nicht Gesetzesadressat, es treffen ihn keine gesetzlichen Informationspflichten und er kann nicht auf dem Verordnungsweg in Pflicht genommen werden. Eine Informationspflicht des Auftragsdatenbearbeiters würde seiner Weisungsbindung widersprechen. Art. 19 revDSG geht klar von der Alleintragung des Verantwortlichen aus, insofern hier die Grenzen zum Auftragsdatenbearbeiter verwischt werden. Vielmehr steht der Verantwortliche in der Pflicht, durch Auswahl und Instruktion des Auftragsbearbeiters für eine entsprechende Erfüllung von Art. 19 revDSG zu sorgen. Abs. 1 äussert sich weiter zur Ausgestaltung der Informationspflicht. Leider wird im erläuternden Bericht nicht klargestellt, dass eine Datenschutzerklärung auf der Website in der Regel genügt – im Gegenteil. Auch enthält der erläuternde Bericht praxisfremde Empfehlungen (z.B. eine Empfehlung, am Telefon den Link zur Datenschutzerklärung zu nennen). Abs. 1 in Kombination mit den Erläuterungen ist gesamthaft unpräzise, führt zu Rechtsunsicherheit und es fehlt an einer Auseinandersetzung mit den wesentlichen Fragen in diesem Bereich.

Die Bestimmung in Abs. 2 ist ersatzlos zu streichen: Der EDÖB hat keine gesetzliche Regelungskompetenz bei der Ausgestaltung von Piktogrammen. Die Entwicklung von Piktogrammen ist Sache der Verantwortlichen. Die vorgeschlagenen Vorgaben würden die Einführung der aus Datenschutzsicht grundsätzlich vorteilhaften Piktogramme unnötig erschweren oder gar verhindern. Die «Maschinenlesbarkeit» ist ein irritierendes Kriterium, für das es keinen Standard gibt. Gesamthaft fehlt es der Norm an der gesetzlichen Grundlage, und es ist offengelassen, ob eine Strafbarkeit möglich ist.

- Art. 14 E-VDSG Informationspflicht der Bundesorgane bei der systematischen Beschaffung von Personendaten (Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters): *Präzisierung.*

Die Bestimmung sieht vor, dass das verantwortliche Bundesorgan bei der systematischen Beschaffung von Personendaten die betroffene Person auf die Freiwilligkeit der Auskunftserteilung hinweist, falls diese zur Auskunft nicht verpflichtet ist. Diese Bestimmung ist praxisfremd, da die Freiwilligkeit häufig aus den Umständen hervorgeht. Entsprechend ist der Wortlaut zu ergänzen mit « (...) soweit dies nicht aus den Umständen ersichtlich ist».

- Art. 15 E-VDSG Information bei der Bekanntgabe von Personendaten (Pflichten des Verantwortlichen): *Streichen.*

Bei der Bekanntgabe von Personendaten muss der Empfänger gemäss dieser Bestimmung über Aktualität, Zuverlässigkeit und Vollständigkeit der bekanntgegebenen Daten informiert werden. Der Einbezug des Auftragsarbeiters ist wiederum nicht vom revDSG abgedeckt (fehlende gesetzliche Grundlage) und die Bestimmung ist nicht praktikabel. Letztlich ist es Sache des Verantwortlichen, die Einhaltung der Datenschutzgrundsätze sicherzustellen. Dieser kann eine Angabe der Aktualität und dergleichen von Personendaten verlangen, aber nicht in allen Fällen. Eine harte Pflicht zu einer solchen Information kann in der Praxis nicht umgesetzt werden. Zudem wäre auch das wieder ein Swiss Finish.

- Art. 16 E-VDSG Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten (Pflichten des Verantwortlichen): *Streichen oder eventualiter Begrenzung der Mitteilungspflicht auf weitergegebene Daten.*

Gemäss dieser Bestimmung informiert der Verantwortliche den Empfänger von bekanntgegebenen Personendaten unverzüglich über Berichtigung, Löschung, Vernichtung sowie Einschränkung der Bearbeitung von Personendaten. Diese Bestimmung ist ersatzlos zu streichen, da sie im Entwurf zum revDSG zwar vorgesehen, aber durch das Parlament gestrichen wurde. Eine Wiedereinführung auf dem Verordnungstext würde den Willen des Gesetzgebers missachten. Die Bestimmung scheint sich betreffend die Einschränkung der Bearbeitung an Art. 18 der DSGVO anzulehnen, obwohl das revDSG dieses Betroffenenrecht nicht kennt und keine gesetzliche Grundlage dafür anbietet. Die entsprechenden Pflichten werden bereits durch die Bearbeitungsgrundsätze vorgegeben und (via Vertragsvorgaben) an die Empfänger weitergegeben. Bei den heutigen systembedingten Bearbeitungen werden korrigierte/ gelöschte Daten für die Empfänger regelmässig systembedingt aktualisiert, damit die richtigen Daten bearbeitet werden können.

Wird die Bestimmung überarbeitet und beibehalten, so muss die Mitteilungspflicht zwingend auf weitergegebene Daten begrenzt werden. Bei allen anderen Daten erscheint dies nicht sachgerecht, weshalb Art. 16 E-VDSG entsprechend präzisiert werden müsste.

- Art. 19 E-VDSG Meldung der Verletzungen der Datensicherheit (Pflichten des Verantwortlichen): *Streichen Abs. 5.*

Abs. 5 dieser Bestimmung hält Dokumentationspflichten für den Verantwortlichem im Falle einer Verletzung der Datensicherheit fest und macht Vorgaben zur inhaltlichen Ausgestaltung. Leider geht weder aus dem Normtext noch aus den Erläuterungen hervor, wozu diese dient. Aus der Gesetzessystematik ergibt sich grundsätzlich, dass nur Verletzungen zu dokumentieren sind, welche eine Meldepflicht gegenüber dem EDÖB begründen, nicht Verletzungen unterhalb der Meldeschwelle. Abs. 5 hält zudem fest, dass «alle mit den Vorfällen zusammenhängenden Tatsachen» gemeldet werden müssen. Dies ist in der Praxis nicht möglich: Die Dokumentationspflicht kann nur bekannte Fälle abdecken; der Verantwortliche ist nicht gehalten, weitere Nachforschungen anzustellen.

Zudem ist die dreijährige Frist zwecks Dokumentierung unverhältnismässig lange gewählt: Die Frist ist auf ein Jahr zu begrenzen, sollte Abs. 5 nicht gestrichen werden. Der Absatz entbehrt zudem einer gesetzlichen Grundlage im revDSG und ist lediglich aus der DSGVO bekannt.

- Art. 20 E-VDSG Modalitäten (Auskunftsrecht der betroffenen Person): *Anpassen Abs. 1, 3 und 5.*

Abs. 1 hält fest, dass das Auskunftsbegehren schriftlich zu stellen sei und dass, «wenn alle einverstanden sind», das Begehren auch mündlich gestellt werden kann. Diese Regelung ist in der Praxis wenig hilfreich: Ein Auskunftsbegehren kann immer mündlich gestellt werden, nur muss der Verantwortliche bei mündlichen Begehren nicht reagieren. Wenn schon, dann müsste der Wortlaut gemäss unseren Mitgliedern explizit dahingehend ergänzt werden, dass ein Begehren nicht nur schriftlich, sondern auch elektronisch gestellt werden kann. Dies ist zwar bereits in den Erläuterungen zur Verordnung festgehalten, sollte aber aufgrund des hohen Stellenwerts auch im Wortlaut des Artikels selbst klargestellt werden.

Nach Abs. 3 muss die Auskunft für die betroffene Person verständlich sein: Es handelt sich hierbei um einen Swiss Finish und es ist nicht klar, wann eine Auskunft «verständlich» ist. Es stellt sich beispielsweise die Frage, was dem Teilnehmer einer medizinischen Studie erklärt werden muss, der alle von ihm erhobenen Daten anfragt. Ob eine Auskunft verständlich ist, liegt in erster Linie am Empfängerhorizont und es wäre unzumutbar, dass auf besondere Schwächen des konkreten Auskunftsstellers eingegangen werden muss. Massgeblich wäre der Durchschnitts-Betroffene.

Gemäss Abs. 5 hat der Verantwortliche die Dokumentation über die Gründe für eine Verweigerung, einen Aufschub oder eine Einschränkung des Auskunftsrechts mindestens für drei Jahre aufzubewahren. Auch diese Dokumentationsfrist ist unverhältnismässig lange gewählt und ist auf ein Jahr zu begrenzen.

- Art. 21 E-VDSG Zuständigkeit (Auskunftsrecht der betroffenen Person): *Anpassen Abs. 2.*

Diese Norm regelt in Abs. 1 die Zuständigkeit für die Gewährung des Auskunftsrechts bei mehreren Verantwortlichen. Abs. 2 bezieht sich auf Daten, die von einem Auftragsdatenbearbeiter bearbeitet werden: Der Verantwortliche hat ihm das Auskunftsbegehren weiterzuleiten, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen. Besser wäre es unserer Ansicht nach, den Auftragsdatenbearbeiter zu verpflichten, den Verantwortlichen dabei zu unterstützen, die Auskunft zu erteilen. Diese Lösung ist in der Praxis entsprechend vertraglich geregelt. Auftragsbearbeiter sind in der Regel nicht darauf eingerichtet, Auskunft zu erteilen, weil sie keine gesetzliche Pflicht trifft. Der vorliegende Verweis auf den Auftragsbearbeiter kann in der Praxis deshalb Probleme schaffen. Zudem kann ein Verantwortlicher es sich aus Compliance-Gründen nicht leisten, die Auskunft einfach weiterzuleiten statt die notwendigen, internen Prozesse aufzubauen. Leidtragend wären die betroffenen Personen. Die Verpflichtung zur Auskunftserteilung muss klar zugewiesen werden. Der Wortlaut von Abs. 2 ist entsprechend anzupassen.

- Art. 23 E-VDSG Ausnahmen von der Kostenlosigkeit (Auskunftsrecht der betroffenen Person: *Anpassen Abs. 1 i.V.m. Abs. 2.*

Abs. 1 legt eine angemessene Beteiligung an den Kosten fest, wenn die Auskunftserteilung mit unverhältnismässigem Aufwand verbunden ist. Abs. 2 legt die Obergrenze der Beteiligung für die gesuchstellende Person auf CHF 300.- fest. Besonders für kleinere Firmen wäre eine Erhöhung der Obergrenze relevant, da grössere Firmen in der Regel über etablierte Prozesse zwecks Auskunftserteilung ohne erheblichen Mehraufwand verfügen. Zudem fehlt in Abs. 1 die Klarstellung und Ergänzung, dass auch querulatorische Auskunftsbegehren unter die Bestimmung fallen.

- Art. 25 E-VDSG Datenschutzberaterin oder Datenschutzberater: *Klarstellen.*

Die Norm äussert sich zu den Kompetenzen eines privaten Datenschutzberaters und hält fest, welche Ressourcen und Befugnisse der Verantwortliche der privaten Datenschutzberaterin zur Verfügung stellen muss. Leider fehlt die Abstimmung zwischen Gesetz und Verordnung. Das Pflichtenheft wurde nicht aus dem revDSG übernommen, sondern aus der bisherigen Verordnung. Im revDSG werden bereits Schulung, Beratung und Mitwirkung an der Compliance genannt, womit fraglich ist, ob es die entsprechende Regelung in der VDSG überhaupt braucht. Zudem fällt auf, dass die Aufgaben als persönliche gesetzliche Pflicht der privaten Datenschutzberaterin aufgeführt werden, was haftungsrechtliche Fragen ohne entsprechende Klärung nach sich zieht. In den genannten Punkten ist eine Klarstellung bzw. Überarbeitung notwendig.

- Art. 26 E-VDSG Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten: *Klarstellen.*

Gemäss dieser Bestimmung kann der Bundesrat bei Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern Ausnahmen von der Inventarpflicht vorsehen, sofern nicht «umfangreich besonders schützenswerte Personendaten bearbeitet werden» und nicht ein «Profilig mit hohem Risiko» durchgeführt wird. Es ist im Umkehrschluss nicht klar, ob nun nur diese beiden Fälle ein hohes Risiko mit sich bringen. Zudem ist klarzustellen, ob dies auch der Massstab ist, wann eine Datenschutz-Folgenabschätzung durchzuführen ist. Unklar ist auch, ob bei Nichterfüllen einer der genannten Ausnahmen ein Inventar für sämtliche Aktivitäten zu erstellen ist.

- Art. 32 Abs. 1 E-VDSG Meldung an den EDÖB (Projekte von Bundesorganen zur automatisierten Bearbeitung): *Streichen*

Die Bestimmung sieht vor, dass Bundesorgane geplante automatisierte Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung dem EDÖB melden müssen. Dies führt zu einem erheblichen Mehraufwand für die Dokumentation, insbesondere da jede automatisierte Bearbeitung und nicht nur solche mit einem (potenziellen) hohen Risiko gemeldet werden müssen. Weiter sind im vorgesehenen Meldezeitpunkt die verlangten Angaben in aller Regel noch nicht genügend detailliert vorhanden. Nicht zuletzt fehlt der Bestimmung auch die gesetzliche Grundlage im revDSG. Wir beantragen diese Norm zur ersatzlosen Streichung.

- 7. Kapitel Schlussbestimmungen: *Anpassen*

Das Regime der Übergangsbestimmungen auf Stufe revDSG fällt lückenhaft aus, weshalb eine Anpassung auf Verordnungsstufe zu erfolgen hat. Für sämtliche neuen Pflichten, welche erheblichen Aufwand generieren, müssen angemessene Übergangsfristen bestehen. Der etablierte Erfahrungswert für einen angemessenen Zeitraum liegt bei zwei Jahren (analog DSGVO). Im revDSG liegt der Fokus jedoch nicht, wie in der DSGVO, auf Übergangsfristen für das Gesamtpaket, sondern auf einzelnen Regeln und Pflichten.

Im revDSG bestehen einige neue Pflichten, für die keine Übergangsfrist festgelegt wurde: Art. 8 revDSG (Pflicht, eine angemessene Datensicherheit zu gewährleisten), Art. 12 revDSG (Pflicht zur Erstellung eines Datenbearbeitungs-Verzeichnisses) und Art. 24 i.V.m. Art. 19 revDSG (Meldepflicht bei Verletzung der Datensicherheit). Für diese drei Pflichten wäre, unter Berücksichtigung des Erhalts der Äquivalenzanerkennung, eine Übergangsfrist bis mindestens anfangs 2023 notwendig. Die Anpassung in der Verordnung könnte mittels eines neuen, spezifischen Artikels bei den Schlussbestimmungen oder mittels einer Verschiebung des Inkrafttretens des Gesamtpakets (revDSG und E-VDSG) auf anfangs 2023 erreicht werden.

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Andreas Knöpfli
Präsident

Ivette Djonova
Head Legal & Public Affairs