Geschäftsstelle
Swiss Payment Association
Ohmstrasse 11
8050 Zürich
www.swiss-payment-association.ch

Kontakt
Telefon: +41 58 426 25 55
office@swiss-p-a.ch

Swiss Payment Association, Ohmstrasse 11, 8050 Zürich

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
3003 Bern
PER MAIL: jonas.amstutz@bj.admin.ch

Zürich, 11. Oktober 2021

Stellungnahme der Swiss Payment Association (SPA) zur Revision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrter Herr Amstutz

Wir bedanken uns für die Möglichkeit, uns zum Entwurf der totalrevidierten Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG) vernehmen zu lassen. Gerne lassen wir Ihnen hiermit unsere Stellungnahme zukommen.

Vorab gestatten wir uns den Hinweis, dass der Swiss Payment Association (SPA) alle grossen Schweizer Herausgeber[1]von Kreditkarten der internationalen Kartenorganisationen mit gegen 8 Millionen herausgegebenen Karten angehören. Als Branchenorganisation vertritt die SPA die Positionen ihrer Mitglieder im Dialog mit all deren Anspruchsgruppen.

1. Kapitel: Allgemeine Bestimmungen

Das neue Datenschutzgesetz (nDSG) verfolgt einen risikobasierten Ansatz. Auf dieser Grundlage ist der Bundesrat nach Art. 8 Abs. 3 nDSG aufgefordert, Bestimmungen über die Mindestanforderungen an die Datensicherheit zu erlassen. Im 1. Kapitel (Allgemeine Bestimmungen), 1. Abschnitt (Datensicherheit), der E-VDSG finden sich nach Auffassung der SPA jedoch keine derartigen Mindestanforderungen.

[1] Mitglieder der Swiss Payment Association sind die Schweizer Kreditkarten-Herausgeber Cembra Money Bank AG, Cornèr Bank AG, PostFinance AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Payment Services SA.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
1	1	a	Ziel der Bestimmung ist es, Kriterien zu nennen, anhand derselben beurteilt werden kann, ob die technischen/organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessen sind, das von der Datenbearbeitung ausgeht. Unseres Erachtens wird über die meisten der aufgeführten Kriterien jedoch kein Bezug zum Risiko hergestellt, das von einer bestimmten Datenbearbeitung ausgeht.	Es sind Kriterien zu benennen, über die ein Bezug zum Risiko hergestellt werden kann, das von einer konkreten Datenbearbeitung ausgeht (basierend auf Art. 8 Abs. 1 nDSG).
1	1	d	Einerseits ist das Kriterium «Implementierungskosten» unpräzise und damit wenig tauglich. Andererseits erscheint das Kriterium «Implementierungskosten» mit Blick auf die Ausführungen im Erläuternden Bericht als zweitklassig, da es im Bericht stark relativiert wird (es soll nur herangezogen werden dürfen, um zwischen gleichwertigen Massnahmen zur Gewährleistung der Datensicherheit die kostengünstigste wählen zu können). Die vorgenommene Relativierung ist willkürlich und nicht nachvollziehbar.	Anstelle von «Implementierungskosten» sollte der Begriff «Implementierungsaufwand» verwendet werden. Kosten hängen stark von der individuellen Betriebsorganisation ab und fallen dementsprechend für den gleichen Sachverhalt von Betrieb zu Betrieb unterschiedlich aus. Das Kriterium «Kosten» ist daher ungeeignet. Unter den Begriff «Implementierungsaufwand» fallen demgegenüber sämtliche Implementierungs-Aufwendungen bzw. sämtliche für die Implementierung massgeblichen Kostenträger, wie z.B. auch personelle, zeitliche und organisatorische. Es ist klarzustellen, dass die relativierenden Ausführungen im Erläuternden Bericht unzutreffend sind. Denn wenn in Art. 1 Abs. 1 lit. a-d Kriterien zur Beurteilung der Angemessenheit der Massnahmen aufgelistet werden und sich darunter auch das Kriterium der Implementierungskosten befindet, kann dieses den anderen Kriterien nicht nachstehen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
1	2		Die Verpflichtung, die Massnahmen "in angemessenen Abständen" zu überprüfen, führt zu weit. Wenn sich an einer konkreten Datenbearbeitung nichts Wesentliches geändert hat und somit keine neuen Risikofaktoren hinzugekommen sind, ist eine periodische Überprüfung unverhältnismässig. Zudem fehlt es dieser auf Verordnungsstufe eingefügten Verpflichtung an der gesetzlichen Grundlage.	Auf die Pflicht, zur Überprüfung der Massnahmen ist zu verzichten Eventualiter soll die Überprüfung nicht in «angemessenen Abständen», sondern «in angemessener Weise» erfolgen.
2			Es wird verlangt, dass die Massnahmen zur Gewährleistung der Datensicherheit bestimmte Schutzziele «erreichen». Es ist nicht möglich, dass jemand (z.B. der Verantwortliche) garantieren kann, dass bestimmte Ziele erreicht werden. Art. 8 Abs. 2 nDSG verlangt nicht, dass bestimmte Schutzziele zu erreichen sind, sondern dass Verletzungen der Datensicherheit zu vermeiden sind. Einzelne angeführte Schutzziele verlangen Unmögliches bzw. sind überschiessend, zu detailliert oder zu absolut. Gemäss lit. b muss der Zugang «unbefugten Personen verwehrt» werden. Lit. c verlangt, dass unbefugten Personen der Zugriff auf Datenträger «verunmöglicht» wird. Weiter ist in lit. d und in lit. e von «verhindern» die Rede. Und in lit. j wird «gewährleisten» verlangt. Um Praxistauglichkeit zu erreichen, ist eine Reduktion auf das Wesentliche erforderlich. Zu den Schutzzielen wird im Erläuternden Bericht (S. 17) ausgeführt: «Ist ein Schutzziel in einem Fall nicht von Relevanz, so müssen der Verantwortliche und Auftragsbearbeiter aber in der Lage sein, zu begründen, weshalb dies der Fall ist.» Diese Begründungspflicht bei Nicht-Berücksichtigung führt zu einem grossen administrativen Aufwand.	Anstatt Schutzziele zu erreichen, müssen die Massnahmen ermöglichen, Verletzungen der Datensicherheit zu vermeiden. Die Verordnungsbestimmung ist konsequent auf diese gesetzliche Vorgabe auszurichten. Entsprechend den Ausführungen im erläuternden Bericht sollten die Massnahme auf die aufgelisteten Schutzziele «ausgerichtet werden.» Art. 2 Satz 1 könnte wie folgt formuliert werden: «Die Massnahmen zur angemessenen Vermeidung von Verletzungen der Datensicherheit sind, soweit von Relevanz, auf folgende Schutzziele auszurichten:». Der überschiessende Katalog der Schutzziele soll durch die klassischen Schutzziele «Vertraulichkeit», «Integrität» und «Verfügbarkeit» ersetzt werden. Es soll nicht jedes Mal bzw. für jedes nicht verfolgte Schutzziel begründet werden müssen, warum keine Berücksichtigung des Schutzziels stattfinden kann. Vielmehr soll anhand der Datenbearbeitung eruiert werden, welche Schutzziele vernünftigerweise in Frage kommen. Das Resultat dieses Prozesses ist mit kurzer Begründung zu dokumentieren.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
3			Für die in Art. 3 statuierte Protokollierungspflicht gibt es im nDSG keine gesetzliche Grundlage. Ebenso gibt es keine gesetzliche Grundlage für die Aufbewahrungspflicht von zwei Jahren.	Die Protokollierungspflicht ist aus der E-VSDG zu streichen. Im Minimum ist klarzustellen, dass es sich bei der Protokollierung um keine Mindestanforderung an die Datensicherheit handelt. Zudem ist auf die Regelung der Aufbewahrungsdauer, auf die enge Zweckbindung und auf die strenge Zugangsbeschränkung zu verzichten.
4	1 und 2		Für die in Art. 4 Abs. 1 E-VDSG statuierte Pflicht zur Erstellung eines Bearbeitungsreglements gibt es im nDSG keine gesetzliche Grundlage. Weiter ist der Zweck des Bearbeitungsreglements nicht ersichtlich, da private Verantwortliche bereits ein Bearbeitungsverzeichnis führen (siehe Art. 12 nDSG), das teilweise deckungsgleich mit dem vorgesehenen Bearbeitungsreglement ist. Zudem decken bereits die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung sowie die zwingende Offenlegung von automatischen Bearbeitungen, die besonders schützenswerte Personendaten betreffen, alle Anforderungen ab, welche über das Reglement erfüllt werden sollen.	Art. 4 E-VDSG ist ersatzlos zu streichen.
4	3		Art. 4 Abs. 3 statuiert, dass der Verantwortliche das Bearbeitungsreglement der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zu Verfügung stellt. Dazu ist festzuhalten, dass sich aus dem nDSG keine Pflicht zur Ernennung einer Datenschutzberaterin/eines Datenschutzberaters ergibt, womit auch keine Verpflichtung bestehen kann, die Beraterin oder den Berater mit einem Reglement zu versehen. Zudem ist nicht klar, was mit «in verständlicher Form» gemeint ist.	Art. 4 E-VDSG ist ersatzlos zu streichen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
6	1		Art. 6 Abs. 1 verlangt, dass der Verantwortliche «sicherstellt», dass ein Auftragsbearbeiter die Daten vertrags- oder gesetzesgemäss bearbeitet. Diese absolute Formulierung führt zu weit und ist realitätsfern. Art. 9 nDSG statuiert eine datenschutzrechtliche Sorgfaltspflicht des Verantwortlichen, verlangt aber zu Recht kein «Sicherstellen», dass der Auftragsbearbeiter die Daten vertrags- oder gesetzesgemäss bearbeitet (denn das kann der Verantwortliche nicht sicherstellen bzw. nicht garantieren). Es fehlt damit an einer gesetzlichen Grundlage für die Pflicht zur Sicherstellung einer gesetzes- und vertragskonformen Datenbearbeitung. Der erste Satz von Art. 6 Abs. 1 wiederholt einerseits eine Banalität und ist anderseits ungenau, da er den falschen Eindruck erweckt, dass die Verantwortlichkeit des Verantwortlichen in keinem Fall eingeschränkt ist, auch dann nicht, wenn ihm nichts vorgeworfen werden kann. Dem ist jedoch nicht so. Es ist ohnehin nicht klar, was «für den Datenschutz verantwortlich» meint. 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. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR.	Mit Blick auf die fehlende gesetzliche Grundlage und die unklare bzw. einen falschen Eindruck erweckende Formulierung ist Abs. 1 von Art. 6 ersatzlos zu streichen.
6	2		Die Bekanntgabe von Personendaten ins Ausland ist in der E-VDSG in Art. 8 ff. (und im nDSG in Art. 16 ff.) geregelt, weshalb Absatz 2 von Art. 6 E-VSDG einerseits systematisch falsch ist und andererseits keine materielle Notwendigkeit dafür besteht. Denn Art. 16 f. nDSG und Art. 9 Abs. 1 nDSG regeln diesen Sachverhalt bereits abschliessend (und Art. 6 Abs. 2 E-VDSG steht damit im Konflikt).	Absatz 2 von Artikel 6 E-VDSG ist ersatzlos zu streichen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
6	3		Wie an anderen Orten im Erläuternden Bericht ausgeführt (siehe S. 35/87), sollte auch hier – am besten im Verordnungstext selbst – präzisiert werden, dass unter «schriftlich» alle Formen (auch elektronische/digitale) fallen, die den Nachweis durch Text ermöglichen (z.B. ein E-Mail).	Es ist in der E-VDSG klarzustellen, dass unter «schriftlich» alle (physischen und elektronischen/digitalen) Formen fallen, die den Nachweis durch Text ermöglichen.
8	3		Es ist davon auszugehen, dass in Abs. 3 von Art. 8 der Bundesrat angesprochen ist; d.h. ihm (und nicht etwa dem Verantwortlichen) obliegt die Pflicht, die Angemessenheit des Datenschutzes des ausländischen Staates etc. periodisch neu zu beurteilen.	Mindestens der Wortlaut von Art. 8 Abs. 3 ist dahingehend zu präzisieren, dass die Pflicht zur periodischen Neubeurteilung dem Bundesrat obliegt. Noch besser wäre, wenn diese Klärung (Adressat der Bestimmung ist der Bundesrat) für den gesamten Artikel 8 vorgenommen würde.
8	6		Es ist das Verständnis, dass der EDÖB vom Bundesrat vor jedem Entscheid über die Angemessenheit des Datenschutzes von Drittstaaten konsultiert wird.	Der Wortlaut von Art. 8 Abs. 6 ist dahingehend zu präzisieren, dass die Konsultationspflicht nicht dem Verantwortlichen im Einzelfall obliegt, sondern dem Bundesrat im Rahmen dessen genereller Beurteilung der einzelnen Länder etc. Noch besser wäre, wenn generell klargestellt würde, dass sich Art 8 E-VDSG in seiner Gesamtheit an den Bundesrat richtet.
9	1		Die Aufzählung der Anforderungen an Datenschutzklauseln ist untauglich, weil sie nicht zwischen der Art der Übermittlung bzw. Rollen des Exporteurs und Importeurs unterscheidet. Diese sind jedoch für den Inhalt des Vertrags entscheidend, wie beispielsweise die vom EDÖB inzwischen anerkannten Standardvertragsklauseln der Europäischen Kommission (EU SCC) zeigen. So macht es keinen Sinn, Auftragsbearbeiter im Ausland zur Anwendung der Bearbeitungsgrundsätze, zur Information der betroffenen Personen oder zur Wahrung der Rechte der betroffenen Personen zu verpflichten. Sie müssen dem nach nDSG nicht nachkommen, weshalb nicht einzusehen ist, dass sie hierzu vertraglich verpflichtet werden sollen. Zudem fehlt in den Bearbeitungsgrundsätzen (lit. a) der Grundsatz der Transparenz.	Der Anforderungskatalog von Art. 9 Abs. 1 E-VDSG ist ersatzlos zu streichen. Im Minimum ist er anzupassen (siehe auch nachstehend), um unterschiedliche Konstellationen (Controller, Processor) abzudecken. Dabei wäre auch das «mindestens» durch «je nach den Umständen» zu ersetzen. Lit. a ist um den Grundsatz der Transparenz zu erweitern.

			Keine rechtliche Grundlage hat das Erfordernis in lit. d und e, den Namen der Staaten oder der internationalen Organe zu nennen, denen Personendaten bekanntgegeben werden, soweit hiermit Weiterübermittlungen gemeint sind, was nicht klar ist. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Lit. f ist bereits über den Grundsatz der Verhältnismässigkeit abgedeckt und damit redundant. 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. Es fehlen Regelungen zur Meldung von Verletzungen der Datensicherheit, insbesondere soweit die betroffenen Personen zu informieren sind.	Lit d, e, f und g sind ersatzlos zu streichen. Schliesslich sind Meldungen betreffend eine Verletzung der Datensicherheit sind zu regeln.
9	2		In Art. 9 Abs. 2 wird die Pflicht statuiert, dass der Verantwortliche «sicherstellen» muss, dass der Empfänger die Datenschutzklauseln einhält. Diese absolute Formulierung führt zu weit bzw. ist realitätsfern, da der Verantwortliche die Einhaltung der Datenschutzklauseln nicht sicherstellen bzw. nicht garantieren kann.	Das Verb «sicherstellen» ist zu ersetzen, z.B. durch die Formulierung »Der Verantwortliche trägt mit angemessenen Massnahmen Sorge dafür, dass…»
10	1		In Absatz 1 ist verlangt, dass der Verantwortliche «sicherstellt», dass Datenschutzklauseln von den Empfängern der Daten beachtet werden. Diese Beachtung der Klauseln kann der Verantwortliche nicht sicherstellen. Im Erläuternden Bericht wird auf Seite 28/87 ausgeführt, dass Daten-Empfänger „die schweizerischen Datenschutzvorschriften“ einhalten müssen. Die Beachtungspflicht kann sich jedoch nur auf die Einhaltung der Standarddatenschutzklauseln beziehen. Darüber hinaus kann es nur um die Einhaltung von Bestimmungen gehen, die einen gleichwertigen Datenschutz wie in der Schweiz gewährleisten (siehe die Formulierung in Art. 6 Abs. 2 E-VDSG).	Vom Verb «sicherstellen» ist Abstand zu nehmen. Ein möglicher Ersatz könnte «hinwirken» sein oder Sorge tragen» bzw. «dafür sorgen» (analog zur aktuellen Formulierung in Art. 22 Abs. 2 VDSG). Alternativ könnte eine Formulierung gewählt werden, wonach der Verantwortliche angemessene Massnahmen zur Einhaltung der Standardschutzklauseln durch die Datenempfänger treffen muss. Bezüglich Einhaltung der schweizerischen Datenschutzvorschriften ist klarzustellen, dass die Standarddatenschutzklauseln und die Bestimmungen, die einen gleichwertigen Datenschutz wie in der Schweiz gewährleisten, einzuhalten sind (und nicht die schweizerischen Datenschutzvorschriften).

2. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
13	1		Für die in Art. 13 Abs. 1 E-VDSG statuierte Informationspflicht des Auftragsbearbeiters gegenüber der von Datenbeschaffung betroffenen Person gibt es keine gesetzliche Grundlage. Nur dem Verantwortlichen der Datenbearbeitung obliegt eine Informationspflicht. (Art. 19 nDSG). Art. 19 nDSG verlangt eine Information der betroffenen Personen, nicht eine Mitteilung. Für eine Information der betroffenen Person genügt ein Zugänglichmachen. Dies entspricht auch dem Verständnis unter der DSGVO. Durch die Wortwahl «mitteilen» darf keine Verschärfung impliziert werden. Gemäss Verordnungstext sind die Informationen über die Beschaffung von Personendaten in «leicht zugänglicher Form» mitzuteilen. Zugunsten der Rechtssicherheit ist hier in dem Sinne eine Konkretisierung des Verordnungstextes erwünscht, dass als «leicht zugänglich» insbesondere auch die Publikation auf einer Website gilt. In diesem Sinne ist klarzustellen, dass der Erläuternde Bericht fehl geht, wenn darin erwähnt wird, dass eine Kommunikation über eine Website nicht immer genüge. Die im Erläuternden Bericht gemachten Ausführungen sind praxisfremd.	Mangels gesetzlicher Grundlage ist von der in Art. 13. Abs. 1 statuierten Informationspflicht des Auftragsbearbeiters Abstand zu nehmen. Anpassungsvorschlag: «Der Verantwortliche ~~und der Auftragsbearbeiter teilen~~*stellt* die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form *zur Verfügung*~~mit~~. *Als leicht zugänglich gilt eine Information insbesondere dann, wenn sie auf der Webseite des Verantwortlichen abrufbar ist.* ~~Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.~~»
13	2		Einerseits ist nicht klar, was mit der «Maschinenlesbarkeit von Piktogrammen» gemeint ist, anderseits führt Art. 13 Abs. 2 für die Piktogramme mit der Maschinenlesbarkeit ein neues Formerfordernis ein, für das es keine gesetzliche Grundlage gibt (das nDSG sieht keine Formerfordernisse für Informationen vor).	Mangels gesetzlicher Grundlage und infolge Unverständlichkeit ist Absatz 2 von Art. 13 ersatzlos zu streichen.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
15			Für die in Art. 15 statuierte Pflicht fehlt es in zweierlei Hinsicht an der gesetzlichen Grundlage. Zum einen auferlegt das nDSG – wie bereits vorstehend erwähnt – dem Auftragsbearbeiter keine Informationspflicht. Zum anderen sieht das nDSG nicht vor, dass den Empfängern von Personendaten Informationen zur Aktualität, Zuverlässigkeit und Vollständigkeit der Daten mitgeteilt werden müssen. Zudem ist unklar, was mit «Zuverlässigkeit» der Personendaten gemeint ist.	Art. 15 E-VDSG ist ersatzlos zu streichen.
16			Für die in Art. 16 statuierten Informationspflichten gibt es nicht nur keine gesetzliche Grundlage im nDSG. Vielmehr waren die in Art. 16 der Verordnung enthaltenen Pflichten Bestandteil des Vorentwurfs zum totalrevidierten DSG, wurden aber im Rahmen des Vernehmlassungsverfahrens bewusst gestrichen. Es ist daher nicht korrekt, sie nun auf Verordnungsstufe wieder einzuführen.	Art. 16 E-VDSG ist ersatzlos zu streichen.
18			Es besteht eine grosse Unsicherheit, darüber, bei welchen Bearbeitungen eine Datenschutz-Folgeabschätzung (DSFA) erforderlich ist und bei welchen nicht. Über die VDSG sollte hier mehr Klarheit geschaffen werden. Denkbar wäre, dass analog zu Art. 35 Abs. 4 DSGVO der EDÖB eine Liste publiziert, welche die Bearbeitungen enthält, für die eine oder für die keine DSFA vorzunehmen ist. Alternativ könnte die VDSG Kriterien nennen, die es erlauben zu ermitteln, ob eine DSFA durchgeführt werden muss oder nicht. Wie an anderen Orten im Erläuternden Bericht ausgeführt (siehe S. 35/87), sollte auch hier – am besten im Verordnungstext selbst – präzisiert werden, dass unter «schriftlich» alle Formen (auch elektronische/digitale) fallen, die den Nachweis durch Text ermöglichen. Für die Aufbewahrungsfrist der DSFA gibt es keine gesetzliche Grundlage, weshalb auf die Frist zu verzichten ist.	Formulierungsvorschlag: «[1] *Der EDÖB veröffentlicht eine Liste mit Bearbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Er kann zusätzlich eine Liste mit Bearbeitungsvorgängen veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.* [2] Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich oder *in einer anderen Form, die den Nachweis durch Text ermöglicht, festhalten.* ~~Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.~~»

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
19			Art. 19 E-VDSG basiert auf Art. 24 nDSG. Zu melden sind demnach Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Die gesetzliche Einschränkung auf Verletzungen, die zu einem hohen Risiko für die Persönlichkeit/die Grundrechte führen, sollte auch in der Verordnungsbestimmung anklingen. Im Erläuternden Bericht finden sich auf Seite 32/87 Ausführungen dazu, was unter «voraussichtlich» (gemäss Art. 24 Abs. 1 nDSG) verstanden werden soll und welches die Folgerungen daraus sind. Dabei wird die Auffassung vertreten, dass bei Verletzungen der Datensicherheit «auch in Zweifelsfällen, in welchen das Vorliegen eines hohen Risikos nicht ausgeschlossen werden kann, eine Meldung zu erfolgen hat.» Diese Interpretation gibt nach Auffassung der SPA den Willen des Gesetzgebers nicht korrekt wieder. «Voraussichtlich» meint vielmehr, dass die Verletzung der Datensicherheit mit höchster Wahrscheinlichkeit zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.	Der Verordnungstext ist dahingehend zu präzisieren, dass Verletzungen der Datensicherheit nur dann gemeldet werden müssen, wenn sie voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Formulierungsvorschlag: «Der Verantwortliche meldet dem EDÖB bei einer *meldepflichtigen* Verletzung der Datensicherheit:» Es ist – im Gegensatz zu den Ausführungen im Erläuternden Bericht – klarzustellen, dass Verletzungen der Datensicherheit nur dann gemeldet werden müssen, wenn die Verletzung höchstwahrscheinlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt – nicht aber dann, wenn ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person nicht ausgeschlossen werden kann.
19	1		Art. 24 nDSG hält fest, dass der Verantwortliche in der Meldung mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen nennt. Dies bedeutet, dass der Verantwortliche zwar zusätzliche Angaben machen kann, aber nicht muss. Den gesetzlichen Anforderungen ist mit der Nennung der Art der Verletzung der Datensicherheit, deren Folgen und der ergriffenen oder vorgesehenen Massnahmen Genüge getan. Es gibt damit keine gesetzliche Grundlage, um auf Verordnungsebene den Katalog der mitzuteilenden Angaben zu erweitern. Überdies ist lit. e falsch formuliert: Die «allfälligen Risiken» beinhalten bereits die Folgen für die	Die in Abs. 1 lit. b-d zusätzlich verlangten Angaben sind aus dem Verordnungstext zu entfernen. Lit. e von Art, 19 Abs. 1 ist wie folgt neu zu formulieren: «die Folgen *der Datenbearbeitungen* für die

			betroffenen Personen. Richtig müsste es heissen «die Folgen der Datenbearbeitungen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht». Auch in lit. f müsste 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). Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB nicht wirklich etwas tun kann oder will (z.B. eine problematische E-Mail geht an den falschen Empfänger und ein Missbrauch durch diesen ist möglich). Damit können auch die Ressourcen des EDÖB geschont werden.	betroffenen Personen, *von welchen ein hohes Risiko ausgeht*» Es sollte zudem eine «de minimis»-Regelung vorgesehen werden, welche Fälle erfasst, in denen trotz eines hohen Risikos für eine betroffene Person sinnvollerweise nicht gemeldet werden muss.
19	3		Art. 24 Abs. 4 nDSG verlangt, dass der Verantwortliche die betroffene Person informiert, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Eine Information an die betroffene Person ist damit nur in den beiden genannten Fällen gesetzlich verlangt. Dagegen wird in Abs. 3 von Art. 19 E-VDSG ohne Einschränkungen verlangt, dass betroffene Personen zu informieren sind. Für diese Ausweitung der Informationspflicht fehlt es an der gesetzlichen Grundlage, weshalb davon Abstand zu nehmen ist.	In Abs. 3 von Art. 19 E-VDSG ist die Informationspflicht wie folgt einzuschränken: «~~Der Verantwortliche teilt den betroffenen Personen~~ *Wenn der Verantwortliche verpflichtet ist, die betroffenen Personen zu informieren, teilt er ihnen* in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 ~~Buchstaben a, e, f und g~~ mit.
19	5		Für die in Abs. 5 postulierte Dokumentationspflicht und für die Aufbewahrungspflicht gibt es keine gesetzliche Grundlage, weshalb darauf zu verzichten ist. Die gesetzliche Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten ist genügend.	Abs. 5 von Art. 19 E-VDSG ist ersatzlos zu streichen.

3. Kapitel: Rechte der betroffenen Person

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
20	1 und 2		Im Erläuternden Bericht wird ausgeführt (siehe S. 35/87), dass zur schriftlichen Form auch die elektronische Form gehört. Das sollte im Verordnungstext selbst präzisiert werden, indem explizit festgehalten wird, dass unter «schriftlich» alle Formen fallen, die den Nachweis durch Text ermöglichen (so z.B. auch ein E-Mail). Der Erläuterungsbericht erwähnt zudem die «digitale Form» ohne klarzustellen, ob diese als «elektronische Form» i.S. von «schriftlich» verstanden wird. Hierzu bedarf es einer Klärung.	Vorgeschlagene Ergänzung: «schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht» Es ist eine Klärung des Begriffs «digitale Form» vorzunehmen.
20	2		Zur Präzisierung sollte in Abs. 2 von Art. 20 E-VDSG festgehalten werden, dass die Einsichtnahme vor Ort auch dann eine gültige Erfüllung der Auskunftspflicht des Verantwortlichen darstellt, wenn aufgrund von berechtigten Interessen des Verantwortlichen eine schriftliche Auskunft nicht zumutbar ist. Im Erläuternden Bericht (S. 35/87) wird ausgeführt, dass die betroffene Person bei der Einsichtnahme an Ort und Stelle gleichwohl die Möglichkeit haben müsse, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Dies entspricht jedoch nicht den Intentionen des Gesetzgebers, wonach im Rahmen des Auskunftsrechts kein Anspruch auf Herausgabe von Akten besteht. Der Gesetzgeber hat die Auskunftspflicht bewusst auf die Mitteilung der „bearbeiteten Personendaten als solche“ (Art. 25 Abs. 2 lit. b nDSG) beschränkt. Damit wird die Auskunftserteilung in aggregierter Form ermöglicht. Dies sollte in der VDSG ausdrücklich festgehalten werden.	Präzisierung von Art. 20 Abs. 2 in dem Sinne, dass die Einsichtnahme vor Ort eine gültige Erfüllung der Auskunftspflicht des Verantwortlichen darstellt. Es ist – im Gegensatz zu den Ausführungen im Erläuternden Bericht – klarzustellen, dass die betroffene Person bei der Einsichtnahme an Ort und Stelle keinen Anspruch auf Herausgabe von Akten bzw. auf das Anfertigen von Fotokopien bestimmter Akten in ihrem Dossier hat. In der VDSG ist ausdrücklich festzuhalten, dass die Auskunftspflicht auf die Mitteilung der bearbeiteten Personendaten als solche beschränkt ist.

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
20	3		Die Anforderung, wonach die Auskunft für die betroffene Person verständlich zu sein hat, ergibt sich bereits aus dem allgemeinen Grundsatz von Treu und Glauben, womit sie im Verordnungstext obsolet ist.	Abs. 3 von Art. 20 E-VDSG ist ersatzlos zu streichen. Eventualiter ist zu präzisieren, dass die Anforderung, wonach die Auskunft für die betroffene Person verständlich zu sein hat, an einem objektiven Massstab zu messen ist. Subjektive Umstände der betroffenen Person dürfen keine Rolle spielen.
20	5		Für die in Abs. 5 von Art. 20 E-VDSG statuierte Dokumentationspflicht fehlt es an der gesetzlichen Grundlage, womit auf diese Pflicht zu verzichten ist. Dies gilt umso mehr, als der Verantwortliche seine Einschränkungsgründe bereits gestützt auf Art. 26 Abs. 4 nDSG gegenüber den betroffenen Personen angeben muss. Um sich im Falle einer Klage oder einer Anzeige zu verteidigen, wird er diese auch aufbewahren.	Absatz 5 von Artikel 20 E-VDSG ist ersatzlos zu streichen.
22			Es ist in der Verordnung klarzustellen, wann die Auskunftserteilungs-Frist von 30 Tagen zu laufen beginnt. Dabei sind u.a. folgende Fälle zu berücksichtigen: • Die Frist beginnt nicht mit Eingang des Begehrens zu laufen, sondern erst wenn der Antragsteller einwandfrei identifiziert werden konnte (wenn z.B. eine Ausweiskopie fehlt, läuft die Frist noch nicht). • Die Frist beginnt erst zu laufen, wenn das Begehren keiner Präzisierung mehr bedarf. Wenn aus dem Auskunftsbegehren beispielsweise nicht hervorgeht, um welche Daten es dem Betroffenen geht und der Verantwortliche um Klarstellung ersucht, beginnt die Frist erst nach erfolgter Klarstellung zu laufen. • Wenn die Auskunftserteilung nicht kostenlos erfolgen kann (Art. 23 Abs. 1 E-VDSG), muss die betroffene Person vor der Auskunftserteilung über die Höhe der Kostenbeteiligung in Kenntnis gesetzt werden (Art. 23 Abs. 3 E-VDSG). Sie kann dann ihr	In Artikel 22 E-VDSG ist klar zu bezeichnen, wann die dreissigtägige Frist für die Auskunftserteilung zu laufen beginnt.

			Gesuch innert zehn Tagen zurückziehen. Die Frist von 30 Tagen für die Auskunftserteilung beginnt damit erst nach Ablauf der Rückzugsfrist zu laufen.	
23	2		Gemäss Art. 25 Abs. 6 nDSG kann der Bundesrat eine Beteiligung an den Kosten der Auskunftserteilung vorsehen, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist. Bereits «normale» Auskunftsbegehren (also solche, die keinen unverhältnismässigen Aufwand im Sinne des Gesetzgebers verursachen) dürften regelmässig einen Aufwand verursachen, der deutlich über dem Betrag vom CHF 300 liegt, der in Art. 23 Abs. 2 E-VDSG vorgesehen ist. Das bedeutet, dass über das Normale hinausgehende Begehren rasch einmal einen Aufwand von vielen tausend oder zehntausend Franken verursachen können. Hierfür nur eine Kostenbeteiligung von CHF 300 vorzusehen, wird der gesetzlichen Bestimmung von Art 25 Abs. 6 nDSG nicht gerecht, da der Kostendeckel in keinem vernünftigen Verhältnis zum effektiven Aufwand steht. Die vorgesehene starre Begrenzung bei CHF 300 ist daher durch eine Regelung zu ersetzen, welche den im Einzelfall konkret anfallenden Kosten besser bzw. angemessen gerecht wird.	Die Beteiligung der betroffenen Person an den Kosten der Auskunftserteilung ist in der VDSG im Verhältnis zum für die Auskunftserteilung angefallenen Aufwand zu regeln. Formulierungsvorschlag: «Die Angemessenheit der Kostenbeteiligung misst sich am tatsächlich für die Auskunftserteilung entstandenen Aufwand»
24			Die Datenportabilität wurde erst in der parlamentarischen Beratung ins nDSG eingefügt. Art. 28 nDSG ist dabei insofern im DSG sachfremd, als damit keine datenschutzrechtlichen Interessen verfolgt werden. Die in Art. 24 E-VDSG vorgesehene analoge Anwendung der Art. 20 bis 23 E-VDSG auf die Datenherausgabe und die Datenübertragung ist daher nicht passend bzw. greift zu kurz.	Von den in Artikel 24 E-VDSG vorgenommenen Verweisen ist abzusehen. Wo nötig sind spezifische bzw. eigenständige Ausführungsbestimmungen zur Datenportabilität zu erlassen.

4. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
25			Die Kompetenzen des Datenschutzbeauftragten nach DSGVO und des Datenschutzberaters nach nDSG/ E-VDSG sind unterschiedlich. Die Abgrenzung zwischen dem Datenschutz*berater* und dem Verantwortlichen ist nicht klar, wenn ein Unternehmen nach Art. 37 DSGVO bereits über einen Datenschutz*beauftragten* verfügt.	Es wäre eine Klärung auf Verordnungsstufe für diejenigen Konstellationen sinnvoll, in denen ein Unternehmen bereits über einen Datenschutzbeauftragten nach DSGVO verfügt.
25	1		Aus dem nDSG ergibt sich keine Pflicht zur Ernennung einer Datenschutzberaterin/eines Datenschutzberaters. Die in Art. 25 Abs. 1 enthaltene Formulierung «Die Datenschutzberaterin […] muss folgende Aufgaben wahrnehmen» suggeriert jedoch, dass eine solche Pflicht besteht. Die Formulierung ist daher anzupassen.	Formulierungsvorschlag: «Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen *nimmt* ~~muss~~ folgende Aufgaben *wahr* ~~wahrnehmen~~:»

6. Kapitel: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Art.	Abs.	Bst.	Kritikpunkt / Anregung	Anpassungs-/ Formulierungsvorschlag
45			Wird der EDÖB gegenüber einer privaten Person tätig, so soll er diese vorab über die voraussichtlichen Gebühren für seine Tätigkeit informieren.	Formulierungsvorschlag: «Der Verantwortliche ist über die erwartete Höhe der Gebühren vorab in Kenntnis zu setzen»

Wir danken Ihnen für die Prüfung unserer Ausführungen sowie für die Berücksichtigung unserer Überlegungen und Anliegen. Gerne stehen wir Ihnen für Rückfragen bzw. zur Erläuterung unserer Eingaben zur Verfügung.

Freundliche Grüsse
Swiss Payment Association

Roland Zwyssig
Präsident

Dr. Thomas Hodel
Geschäftsführer