VUD Verein Unternehmens-Datenschutz

Entwurf der Verordnung zum revidierten DSG (gemäss Vernehmlassung vom 23. Juni 2021)

Kommentierung und Anpassungsvorschläge (Fassung vom 13.9.2021)

Vorbemerkungen:

- Zahlreichen Bestimmungen fehlt eine gesetzliche Grundlage[1] oder sie widersprechen gar direkt dem Willen des Gesetzgebers (insbesondere, was die an zahlreichen Stellen neu eingeführten Dokumentationspflichten betrifft). Sie sind daher zu streichen. Das gilt insbesondere im Bereich der Datensicherheit, deren Verletzung zu einer Strafbarkeit führen soll. Die Voraussetzungen hierfür sind in diesen Fällen jedoch nicht erfüllt, weshalb die Bestimmungen ins Leere schiessen.
- Die Verordnung sollte aus Sicht des VUD auf zu detaillierte Bestimmungen verzichten. Die Vielfalt der Bearbeitungsaktivitäten und Situationen ist so gross, dass Details in aller Regel mehr unbeabsichtigte negative Folgen haben als für Rechtssicherheit zu sorgen. Regelungen nach dem Giesskannenprinzip machen im Datenschutz schlicht keinen Sinn, sondern sind kontraproduktiv.
- Es sollten noch Übergangsfristen von 1 Jahr ab Inkrafttreten des revDSG für die Erstellung der Verzeichnisse und – falls darauf entgegen den Anträgen nicht verzichtet wird – auch für das Bearbeitungsreglement vorgesehen werden.
- Es wäre sinnvoll, bei den einzelnen Verordnungsbestimmungen jeweils auf den Artikel der revDSG verwiesen werden, um dessen Konkretisierung es geht.

Gelb und (nur Bundesorgane betreffend) Hellgelb hervorgehoben sind Bestimmungen, in denen Anpassungsbedarf besteht.

---

[1] «Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die **Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.**» (BGE 141 II 169, E. 3.3).

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
1 Abs. 1	Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien: a. Zweck, Art, Umfang und Umstände der Datenbearbeitung; b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen; c. der Stand der Technik; d. Implementierungskosten.	Der Grundsatz, dass Verantwortliche und Auftragsbearbeiter eine dem Risiko angemessene Datensicherheit gewährleisten müssen, wird hier aufgegriffen (Art. 8 Abs. 1 revDSG). Zu Abs. 1: Massnahmen zur Datensicherheit sind nicht «angemessen», sondern «geeignet», wie dies Art. 8 Abs. 1 revDSG auch sagt. «Angemessen» kann nur das resultierende Sicherheitsniveau sein. Man sollte deshalb auch in Art. 1 Abs. 1 von «geeigneten» Massnahmen sprechen, um terminologische Widersprüche zu vermeiden. Zu lit. a): je höher der Schutzbedarf, desto höher sind auch die Anforderungen an die Massnahmen (z.B. bei besonders schützenswerten Personendaten, oder bei vollständig automatisierter Bearbeitung). Zu lit. b): die Anforderungen an die Massnahmen sind höher, wenn die Eintrittswahrscheinlichkeit höher ist. Zu lit. c): es geht dabei um den gegenwärtige *und* bewährte Techniken, nicht um unerforschte Techniken. Zu lit. d): bei mehreren möglichen Massnahmen darf die kostengünstigste Option gewählt werden. Problematisch ist, dass der Bundesrat von der falschen Vorstellung ausgeht, dass Art. 8 revDSG, der hier konkretisiert wird, mehr als die Datensicherheit i.e.S. regelt (CIA). Es geht weder um Bearbeitungsgrundsätze noch Betroffenenrechte. Die Beispiele in den Erläuterungen sind teilweise falsch. Ob z.B. eine Bearbeitung durch eine KI oder einen Menschen erfolgt, ist für die Frage der Datensicherheit nicht relevant. Ferner ist der Begriff des «Risikos» (Bst. b) falsch formuliert. Zudem geht es hier nicht um das Bruttorisiko, sondern das Nettorisiko. Der Begriff «Implementierungskosten» impliziert, dass anderer Aufwand nicht relevant ist. Das ist falsch. Ebenso falsch ist die Ausführung in der Erläuterung, dass übermässige Kosten nicht	Private Bundesorgane	Statt von «angemessenen» Massnahmen ist von «geeigneten» Massnahmen zu sprechen. Zu schreiben ist: «b. die verbleibenden potenziellen Auswirkungen einer Verletzung der Datensicherheit für die betroffenen Personen und deren Eintrittswahrscheinlichkeit (Restrisiko).» «Implementierungskosten» ist durch «Implementierungsaufwand» zu ersetzen.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		relevant sind. Erforderlich sind nur angemessene Massnahmen, und die Angemessenheit bestimmt sich selbst nach dem Vorschlag auch nach den Kosten.		
1 Abs. 2	Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.	Ist die Gefährdung für die Rechte der Betroffenen grösser, so ist der Abstand der nächsten Prüfung kürzer. Die Formulierung «periodisch» wurde gestrichen. Die Prüfung muss ab einem gewissen Risiko standardisiert erfolgen (Pflicht zur Verwendung von ISO 27001?). Der Fokus auf die «angemessenen Abstände» ist zu eng. Wesentlich ist, dass sie in «angemessener Weise» überprüft werden. Der Begriff des «Abstands» impliziert nach wie vor eine Periodizität, die aber nicht zwingend ist, etwa wenn sich die Umstände nicht verändert haben.	Private Bundesorgane	Statt «angemessenen Abständen» ist «angemessener Weise» zu schreiben.
2	Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen: a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen. b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt. c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht. d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert. e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungs-systemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert.	Es muss nicht zwingend jedes dieser Schutzziele relevant sein, es muss aber begründet werden können, weshalb nicht. Zu lit. b: Der Begriff «Anlage» wurde ergänzt, es sind dabei auch mobile Bearbeitungsanlagen gemeint (z.B. Mobiltelefone oder Tablets). Zu lit. g: auch die Veränderung von Personendaten muss nachträglich überprüfbar sein. Zu lit. h: damit sollen auch die Empfänger der Daten identifiziert werden können (das Organ ist ausreichend). Lit. i, j und k wurden neu eingefügt. Zu lit. i: z.B. die Erstellung eines Backup-Konzepts. Zu lit. j: das System selbst soll automatisch darauf aufmerksam machen, dass eine Fehlfunktion vorliegt. Zu lit. k: der Verantwortliche oder Auftragsbearbeiter muss reaktive Massnahmen treffen zur Minderung der Folgen bei einer Verletzung der Datensicherheit. Die Verwendung des Worts «erreichen» impliziert, dass die Schutzziele vollständig erfüllt werden, was weder erforderlich	Private Bundesorgane	Statt «erreichen» ist «anstreben» zu schreiben. Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden. In diesem Fall wäre die Liste auch konform mit Art. 32 DSGVO.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden. h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden. i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden. j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Dateninteg rität). k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.	noch möglich ist. Zu treffen sind nur angemessene Massnahmen; eine vollständige Sicherheit ist nicht erforderlich. Die aufgeführte Liste ist überdies veraltet, zu absolut und zu detailliert formuliert. Zudem geht es grundsätzlich um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. So ist es auch in Art. 32 Abs. 1 lit. b DSGVO definiert. Die Regelung zwingt zu einer Dokumentation für jede Datenbearbeitung (u.a. warum bestimmte der aufgeführten Schutzziele nicht relevant sind im konkreten Fall). Das widerspricht dem Willen des Gesetzgebers, der eine solche umfassende Dokumentationspflicht abgelehnt hat.		
3 Abs. 1	Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern,	Unternehmen müssen gemäss dem Wortlaut von Art. 3 Abs. 1 E-VDSG Datenbearbeitungen protokollieren, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass trotz der ergriffenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Diese Bestimmung ist in mehrerlei Hinsicht problematisch und sollte ersatzlos gestrichen werden:	Private	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung erreicht das Ziel materiell nicht und zielt an der Sache vorbei.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	Lesen, Bekanntgeben, Löschen oder Vernichten.	*Erstens* fehlt ihr eine gesetzliche Grundlage. Es geht hier nicht primär um die Protokollierung zur Gewährleistung der Datensicherheit, sondern sie dient in erster Linie der *nachträglichen* Feststellung, ob es zu einer unbefugten Bearbeitung des Verantwortlichen bzw. seines Auftragsbearbeiters gekommen ist. Sollen unerlaubte Datenabflüsse, Malware, Einbrüche etc. entdeckt werden, sind andere Dinge zu protokollieren als die reguläre Nutzung der Daten (die Hacker und Malware vermeiden oder löschen werden). Zur Feststellung einer Verletzung der Datensicherheit eignet sie also nicht und ist damit unverhältnismässig. Art. 8 revDSG, welcher als Grundlage der Bestimmung dient, behandelt nur die Datensicherheit i.e.S. Nur solche sollte der Bundesrat gemäss Art. 8 Abs. 3 revDSG ausführen (und nur die Verletzung solcher können auch zu einer Strafbarkeit führen). *Zweitens* ist das Ergebnis der DSFA kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In der Regel wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun. Die Erläuterungen des E-VDSG bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht. *Drittens* muss eine solche Bearbeitung kraft Art. 21 revDSG ohnehin dem EDÖB oder Datenschutzberater vorgelegt werden. Eben dies dient bereits dem Ziel, eine solche oder andere Massnahme vorzuschlagen, soweit die Bearbeitung überhaupt umgesetzt werden kann. Hier pauschal eine spezifische Massnahme ohne Berücksichtigung der Umstände vorzuschlage ist ein Schuss ins Blaue. *Viertens* obliegt die Pflicht auch dem Auftragsbearbeiter, der jedoch die DSFA nicht kennen muss und eine solche schon gar nicht auszuführen hat. Massnahmen zur Datensicherheit obliegen zwar auch ihm, aber diese Protokollierung ist in ihrem Kern keine solche. Das erklärt den unlösbaren Widerspruch. Auch deshalb ist sie zu streichen.		

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Unklar ist aufgrund der Norm, ob eine Protokollierungspflicht auch dann bestehen soll, wenn eine Datenschutz-Folgenabschätzung unterlassen wurde, obwohl sie nötig gewesen wäre. Dies wird aber wohl so sein.		
3 Abs. 2	Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.	Die Pflicht zur Protokollierung besteht unabhängig vom Risiko und muss daher bei jeder automatisierten Bearbeitung von Personendaten vorgenommen werden. Der Begriff der automatisierten Bearbeitung ist nicht definiert. Zu verstehen ist darunter aber das Gegenteil zur manuellen Bearbeitung – somit ist darunter eine elektronische oder vergleichbare Datenbearbeitung zu verstehen. Die Protokollierungen erscheinen als unverhältnismässig – insbesondere, da auch das Lesen protokolliert werden muss. Auch im Falle von Bundesorganen ist die Regelung systematisch falsch und ohne gesetzliche Grundlage. Vgl. dazu die obigen Ausführungen.	Bundesorgan	Streichen (vgl. oben)
3 Abs. 3	Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.	Widerspruch zu den Mindestanforderungen an die Protokollierung gemäss den Absätzen 1 und 2. Abs. 3 bringt allerdings ebenfalls zum Ausdruck, dass es nicht um Verletzungen der Datensicherheit, sondern um etwaige unzulässige Bearbeitungen durch reguläre Benutzer geht. Diese stellen keine solche Verletzungen dar. Mit Empfänger ist die Organisation, nicht die Einzelperson gemeint.	Private Bundesorgane	Streichen (vgl. oben)
3 Abs. 4	Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.	Die Aufbewahrungsfrist von 2 Jahren muss eingehalten werden. Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung der getrennten Aufbewahrung ist technisch nicht ohne Weiteres oder nur mit erheblichem Aufwand umsetzbar. Protokolle werden dort erzeugt, wo sie anfallen – und nicht auf anderen Systemen. Ein Betrieb müsste somit von sämtlichen	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. «getrennt vom System, in welchem die Personendaten bearbeitet werden» ist zu streichen und durch «sicher» zu ersetzen. Die Regelung ist unverhältnismässig.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Protokollen Kopien anfertigen und sie manuell auf ein anderes System übertragen; der Aufbewahrungsort muss ein unabhängiges System sein. Dieser Vorgang birgt seinerseits Sicherheitsrisiken, abgesehen davon, dass der Aufwand enorm wäre Es würde genügen, wenn sichergestellt wird, dass die Protokolle ihrerseits sicher sind. Die Personen, welche die Verletzung von Datenschutzvorschriften verfolgen, erhalten gemäss Wortlaut keinen Zugang zu den Daten. Die Zweckbindung ist unzulässig, da sie strenger ist, als die Bearbeitungsgrundsätze dies erlauben. Damit fehlt der Regelung eine gesetzliche Grundlage. Ein Verantwortlicher oder Auftragsbearbeiter hat möglicherweise ein Interesse, die Logs auch aus anderen Gründen auszuwerten. Tut er dies DSG-konform, sollte dies auch möglich sein. Die Regelung ist insofern interessant, als heute viele Protokolle von IT-Systemen aus Gründen des Datenschutzes weniger lang aufbewahrt werden. Es kann mit Verweis auf den E-VDSG vertreten werden, dass eine Aufbewahrung von zwei Jahren ohne Weiteres verhältnismässig ist, wenn sogar der Gesetzgeber diese Frist standardmässig vorschreiben will. Korrekterweise ist die Aufbewahrungsfrist aber als Mindestfrist auszugestalten. Gibt es Gründe, sie länger aufzubewahren, muss dies möglich sein.		Sofern eine Aufbewahrungsfrist überhaupt festgelegt wird, wofür es keine Grundlage gibt, so macht eine starre Frist keinen Sinn und wäre unverhältnismässig. Sie muss von der Dauer der Datenbearbeitung abhängig und generell angemessen sein. Satz 2 ist zu streichen, da er dem DSG widerspricht, indem er die Bearbeitungsgrundsätze aushebelt. Ohnehin müsste der Personenkreis mit Zugang ist um jene erweitert werden, welche die Verletzung von Datenschutzvorschriften verfolgen.
4 Abs. 1	Bearbeitungsreglement von privaten Personen 1 Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie: a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen.	Die Pflicht, für Datenbearbeitungen mit einem hohen Risiko Bearbeitungsreglemente zu erstellen, besteht bereits nach der geltenden Verordnung. Allerdings wurde allgemein erwartet, auch aufgrund der Botschaft des Bundesrats und der parlamentarischen Beratung, dass die Bearbeitungsreglemente angesichts der neu eingeführten Dokumentations- und Informationspflichten (Verzeichnisse von Bearbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Datenschutzerklärungen) aus der Verordnung gestrichen werden. Das Bearbeitungsreglement dient augenscheinlich nicht der Sicherstellung der Datensicherheit i.e.S., sondern soll primär die	Private	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig und redundant. Es ist ein Swiss Finish.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Einhaltung der Bearbeitungsgrundsätze und die weiteren Vorgaben des Datenschutzes sicherstellen. Es fehlt der Bestimmung somit eine gesetzliche Grundlage, da Art. 8 revDSG nur Datensicherheit i.e.S. regelt. Der Vorgängernorm fehlt ebenfalls die gesetzliche Grundlage, weshalb sie toter Buchstabe blieb bzw. bleiben musste (ihre Verletzung hat keine Rechtsfolgen). Demgegenüber steht der enorme Aufwand, den die Erstellung und Nachführung eines solchen Bearbeitungsreglements mit sich bringt. Wie bei Abs. 2 gezeigt wird, werden die wesentlichen Angaben ohnehin bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar. Die Regelung ist somit überflüssig. Auch die DSGVO sieht eine solche Regelung nicht vor (Swiss Finish). Während ein «Profiling mit hohem Risiko» in der Praxis vermutlich kaum vorkommen wird, stellt sich die Frage, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Dies dürfte mit Bezug auf die HR-Daten bei einem mittleren und grösseren Umfang bereits der Fall sein. Auch jedes Medienunternehmen wird erfasst sein, welches Berichte über Politik und Gesellschaft enthält und damit auch besonders schützenswerte Personendaten (politische Ansichten etc.) bearbeitet. Es ist klar, dass besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern können. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt. Der Erläuterungsbericht suggeriert, dass das Bearbeitungsreglement ein in sich geschlossenes Dokument sein muss. Dies ist praxisfremd und unnötig. Eine solche Pflicht zur «Urkundeneinheit» gilt auch sonst nirgends. Es besteht ferner das Risiko, dass Auskunftsersuchende über die Generalklausel versuchen werden, an das Bearbeitungsreglement heranzukommen.		

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Die Dokumentationspflichten wurden aus der DSGVO übernommen und zusätzlich soll diese bestehende Pflicht nicht gestrichen werden. Dies führt zu einer erheblichen Erweiterung der Dokumentationspflichten.		
4 Abs. 2	Das Reglement muss mindestens Angaben enthalten: a. zum Bearbeitungszweck; b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; d. zur internen Organisation; e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung; f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit; g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe; h. zu den Massnahmen, die zur Datenminimierung getroffen werden; i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung; j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.	Lit. a, b, c und f sind auch Bestandteile der Bearbeitungsverzeichnisse. Die übrigen Punkte müssen bei einer Datenschutz-Folgenabschätzung mitberücksichtigt werden, wenn diese für die Risikoabwägung bzw. als Massnahme zur Reduktion der Risiken relevant sind, was in der Regel der Fall sein wird. Somit sind sie bereits dokumentiert. Die Liste zeigt im Übrigen, dass es augenscheinlich primär nicht um Datensicherheit, sondern die Einhaltung der Bearbeitungsgrundsätze und des restlichen Datenschutzgesetzes geht (s. .	Private	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
4 Abs. 3	Die private Person muss das Reglement regelmässig aktualisieren und der Daten-schutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	Damit wird eine Pflicht zur Vorlage an den Datenschutzberater / die Datenschutzberaterin festgelegt, obwohl keine gesetzliche Verpflichtung besteht, diese Funktion überhaupt zu besetzen. Das Bearbeitungsreglement des Privaten muss weder publiziert noch dem EDÖB gemeldet werden.	Private	Streichen (vgl. oben). In jedem Fall den zweiten Halbsatz streichen.
5 Abs. 1	Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie: a. besonders schützenswerte Personendaten bearbeiten; b. ein Profiling durchführen; c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen; d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen; e. Datenbestände miteinander verknüpfen; oder f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.	Aufgrund der Auflistung muss praktisch für jede automatisierte Bearbeitung ein Reglement erstellt werden. Es ist unklar, warum die Bearbeitungsreglemente trotz Einführung der Verzeichnisse und der Datenschutz-Folgenabschätzung beibehalten werden. Zudem fehlt aus den zu Art. 4 E-VDSG erwähnten Gründen eine gesetzliche Grundlage. Vgl. im Übrigen die obigen Ausführungen zu Art. 4 E-VDSG.	Bundesorgane	Streichen. Es fehlt die gesetzliche Grundlage, die Regelung ist unverhältnismässig.
5 Abs. 2	Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.	Die Formulierung ist unklar: Soll sie bedeuten, dass es allenfalls mehr Angaben enthalten muss?	Bundesorgane	Streichen (vgl. oben)
5 Abs. 3	Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen	Pflicht, das Bearbeitungsreglement dem Datenschutzberater und dem EDÖB bereitzustellen (auf Anfrage).	Bundesorgane	Streichen (vgl. oben)

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
6 Abs. 1	Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.	Der erste Satz wiederholt einerseits eine Banalität, ist andererseits aber 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 ist 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. Dies würde auch über Art. 82 Abs. 3 DSGVO hinausgehen. Für die zivilrechtliche Haftung gilt nach wie vor Art. 41 OR. Die Formulierung «sicherstellen» ist zudem inhaltlich falsch. Der Verantwortliche kann nur «dafür Sorge tragen». Auch der zweite Satz ist mangelhaft, da ihm ebenfalls eine gesetzliche Grundlage fehlt. Nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche 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, aber erlaubt er seinem Auftragsbearbeiter eine Bearbeitung, die noch dem Gesetz entspricht, ist diese Vorschrift bereits verletzt. Gemeint ist vielleicht auch eine Bezugnahme auf Art. 9 Abs. 1 DSG («… Bearbeitung … kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden…). Dies müsste in der Verordnung aber auch nicht wiederholt werden. Die Regel verwirrt also mehr als sie nutzt. Schon nach Art. 9 Abs. 1 Bst. a revDSG hat der Verantwortliche dafür zu sorgen, dass das DSG eingehalten wird. Das genügt.	Private Bundesorgane	Satz 1 streichen, da kein Mehrwert, jedoch verwirrend und falls als Kausalhaftung verstanden ohne gesetzliche Grundlage. Ohnehin ist «sicherstellen» durch «dafür Sorge tragen» zu ersetzen. Satz 2 streichen, da kein Mehrwert, jedoch verwirrend und ohne gesetzliche Grundlage, was die Pflicht zur Vertragsdurchsetzung betrifft.
6 Abs. 2	Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmun-	Der Sinn und Zweck dieser Regelung erschliesst sich nicht, da der Regelungsgehalt bereits durch die Art. 16 und 17 revDSG (Bekanntgabe von Personendaten ins Ausland) gedeckt ist. Gemäss Erläuterungsbericht entspricht der neue Art. 6 Abs. 2 E-VDSG dem geltenden Art. 22 Abs. 3 VDSG. Dabei handelt	Private Bundesorgane	Streichen. Die Regelung steht im Konflikt mit Art. 16 f. revDSG und Art. 9 Abs. 1 Bst. a revDSG, welche

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	gen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.	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 (oder warum es sie überhaupt braucht bzw. auf welche Rechtsgrundlage sie sich stützt). Die Regelung würde nur dort halbwegs Sinn machen, wo ein Schweizer Verantwortlicher einen ausländischen Auftragsbearbeiter bemüht 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. Es ist dies ein absoluter Sonderfall. Eine eigene Regelung in der VDSG rechtfechtfertigt sich dadurch nicht. Die Regelung ergibt sich im übrigen sowieso bereits aus Art. 9 Abs. 1 Bst. 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. Es geht darum sicherzustellen, dass die Daten nur so bearbeitet werden, wie der Verantwortliche dies darf – und so steht es schon in Art. 9 Abs. 1 Bst. a revDSG. Es ist allerdings zweifelhaft, ob die Autoren der Regelung diesen Sonderfall überhaupt im Blick hatten. Vermutlich wurde die Regel einfach übernommen, weil es sie schon gab.		diesen Sachverhalt bereits abschliessend regeln.
6 Abs. 3	Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.	Kern der Regelung ist, dass der Beizug von Unterauftragsbearbeitern im Falle von Bundesorganen *schriftlich* genehmigt werden muss. Das entspricht dem Standard der DSGVO; Art. 9 Abs. 3 revDSG sieht keine Schriftform vor. Hierbei handelt es sich um eine Umsetzung der EU Richtlinie 2016/680 (Justiz und Polizei). Diese verlangt in Art. 22 Abs. 2, dass im öffentlichen Sektor die Zustimmung schriftlich erteilt werden muss. Gemäss Botschaft des Bundesrates zu Art. 8 Abs. 3 E-DSG kann die vorgesehene Genehmigung sowohl im privaten als	Bundesorgane	Klarstellung, dass eine Genehmigung in Textform genügt und sie auch in allgemeiner Form erfolgen kann (beides analog DSGVO).

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		auch im öffentlich-rechtlichen Bereich spezifischer oder allgemeiner Art sein. Die Botschaft führt aus, dass im Falle einer allgemeinen Genehmigung zum Beizug von Subunternehmern, der Auftragsbearbeiter den Verantwortlichen über jede Änderung, wie den Wechsel oder den Beizug neuer Unterauftragsbearbeiter, informieren muss, damit dieser bei Bedarf Einspruch erheben kann. Es ist somit zulässig, dass Behörden ihren Dienstleistern eine grundsätzliche Genehmigung erteilen, Subunternehmer beizuziehen, sofern bei allfälligen Änderungen eine Informationspflicht der Dienstleister besteht und die Behörde ein Vetorecht hat. Wird das Vetorecht ausgeübt, dann führt dies in der Regel bei Standarddienstleistungen zu einem Kündigungsrecht. Gemäss den Erläuterungen zum E-VDSG schliesst die schriftliche Form auch die elektronische Form mit ein. Damit entspricht die Formulierung von Art. 28 Abs. 2 DSGVO, welche ebenfalls «schriftlich» vorschreibt, damit aber auch den Fall des Nachweises durch Text meint. Es sollte ferner klargestellt werden, dass eine allgemeine Genehmigung (analog zur Regelung der DSGVO) zulässig ist, da es Bundesorganen sonst nicht möglich sein wird, Dienste von Standard-Online-Services zu beziehen. Diese verwenden ausschliesslich diese Methode.		
7	Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.	Bundesorgane sind verpflichtet, eine Datenschutzberater*in zu bezeichnen (Art. 27 f DSG). Eine weitere Informationspflicht des Bundesorgans an die Datenschutzberater*in ist bereits in Art. 29 E-VDSG enthalten. Diese ist allgemeiner formuliert und umfasst grundsätzlich auch die Information über Auftragsbearbeitungen, sofern diese relevant sind. Die Formulierung der Norm ist zu salopp. Es ist nicht klar, was «Probleme» sind.	Bundesorgane	Satz 2 ist zu streichen, da unnötig. Jedenfalls ist er präziser zu formulieren.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Die Norm stellt aber klar, dass Art. 28 Abs. 2 lit. a E-VDSG die Datenschutzberater*in *nicht* verpflichtet ist, *jede* Datenbearbeitung zu prüfen; andernfalls wäre eine Information bei Auftragsbearbeitungsverträgen a priori nicht erforderlich.		
8 Abs. 1	Werden Personendaten ins Ausland bekanntgegeben, so müssen 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 berücksichtigt werden: a. die internationalen Verpflichtungen des Staates oder internationalen Organs im Bereich des Datenschutzes; b. die Achtung der Menschenrechte; c. die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung; d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes; e. das wirksame Funktionieren von einer oder mehreren unabhängigen Behörden, die im betreffenden Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.	Hinweis: Dieser Artikel ist an den Bundesrat gerichtet.		
8 Abs. 2	Bei der Beurteilung können die Einschätzungen von internationalen Organen oder ausländischen Behörden, die für den Datenschutz zuständig sind, berücksichtigt werden.	Dieser Artikel ist an den Bundesrat gerichtet.		
8 Abs. 3	Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch neu beurteilt.	Dieser Artikel ist an den Bundesrat gerichtet.		

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
8 Abs. 4	Ergibt sich aus einer Beurteilung nach Absatz 3 oder aus verfügbaren Informationen, dass ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ kein angemessener Datenschutz mehr gewährleistet, so wird der Entscheid gemäss Artikel 16 Absatz 1 DSG geändert, sistiert oder aufgehoben. Dieser neue Entscheid hat keine Auswirkungen auf bereits erfolgte Datenbekanntgaben.	Dieser Artikel ist an den Bundesrat gerichtet.		
8 Abs. 5	Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz sind in Anhang 1 aufgeführt.	Dieser Artikel ist an den Bundesrat gerichtet. Es handelt sich dabei um eine Positiv-Liste. Falls ein Staat nicht aufgeführt ist, heisst das nicht, dass er automatisch über kein angemessenes Datenschutzniveau verfügt, er wurde allenfalls einfach noch nicht geprüft.		
8 Abs. 6	Der EDÖB wird vor jedem Entscheid über die Angemessenheit des Datenschutzes konsultiert.	Dieser Artikel ist an den Bundesrat gerichtet.		
9 Abs. 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 mindestens die folgenden Punkte regeln: a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit; b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen; c. die Art und der 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;	Die spezifischen Garantien müssen im privaten Sektor nicht vom EDÖB genehmigt werden, sondern ihm nur mitgeteilt werden (Art. 16 Abs. 2 lit. b revDSG). Deshalb werden bestimmte Datenschutzstandards an dieser Stelle der Verordnung präzisiert. Die Aufzählung der Anforderungen an einen «Data Transfer Agreement» ist allerdings 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, einen Auftragsbearbeiter im Ausland zur Anwendung der Bearbeitungsgrundsätze, zur Information der betroffenen Personen oder zur Wahrung der Rechte der betroffenen Personen zu verpflichten. Sie müssten dem auch	Private Bundesorgane	Der Anforderungskatalog kann gestrichen werden, da der EDÖB sie sowieso prüfen muss. Wird dies nicht getan, ist der Anforderungskatalog entweder anzupassen, um unterschiedliche Konstellationen abzudecken (Controller, Processor) oder das «mindestens» ist durch «je nach den Umständen» zu ersetzen. Bst. a ist um den Grundsatz der Transparenz zu erweitern. Bst. d, e und f sind zu streichen.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten; g. die zur Bearbeitung der Daten berechtigten 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. die Rechte der betroffenen Person, namentlich: 1. das Auskunftsrecht, 2. das Widerspruchsrecht, 3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten, 4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.	nach revDSG nicht nachkommen, weshalb nicht einzusehen ist, dass sie hierzu vertraglich verpflichtet werden sollen. In den Bearbeitungsgrundsätzen (Bst. a) fehlt der Grundsatz der Transparenz. Keine rechtliche Grundlage hat das Erfordernis in Bst. 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. Es genügt, dass der Empfänger (bzw. Importeur) bezeichnet wird. Auch die EU SCC beschränken sich darauf. Bst. f ist bereits mit dem Grundsatz der Verhältnismässigkeit abgedeckt und damit redundant. Bst. 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.		Meldungen betr. eine Verletzung der Datensicherheit sind zu regeln.
9 Abs. 2	Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.	Der Begriff "sicherzustellen" impliziert eine Garantie der Einhaltung der Klauseln bzw. Kausalhaftung, wofür es keine gesetzliche Grundlage gibt und die vernünftigerweise auch nicht verlangt werden kann.	Private Bundesorgane	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.
9 Abs. 3	Wurde der EDÖB über die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die: a. unter denselben Datenschutzklauseln oder Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck	Diese Bestimmung galt schon bisher.	Private Bundesorgane	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen Unternehmen, die zum selben Konzern gehören, stattfinden, soweit die Datenschutzklauseln oder Garantien weiterhin einen geeigneten Datenschutz gewährleisten.			
10 Abs. 1	Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.	Massnahmen sind angemessen, wenn sie dem Stand der Technik sowie den konkreten Umständen entsprechen. Die Anforderungen an die Massnahmen sind höher, wenn es sich beispielsweise um besonders schützenswerte Personendaten handelt. Wiederum kann der Exporteur nicht «sicherstellen», sondern nur dafür Sorge tragen. Der Erläuterungsbericht verlangt fälschlicherweise, dass der Empfänger verpflichtet werden muss, das Schweizer Datenschutzrecht einzuhalten. Das ist falsch. Einhalten muss er nur den Vertrag. Die Vorschrift führt zu einer Kausalhaftung und ist in der Praxis nicht zu erfüllen. Nicht einmal das Bankenrecht kennt eine derart strenge Regelung. Zudem verlangen die aktuellen Standardvertragsklauseln, die in der Praxis flächendeckend eingesetzt werden, ohnehin entsprechende Sorgfaltspflichten des Exporteurs.	Private Bundesorgane	Der Begriff «sicherstellen» ist durch «in angemessener Weise Sorge zu tragen» zu ersetzen.
10 Abs. 2	Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat.	Die Liste wird auf der Website des EDÖB publiziert.	Private Bundesorgane	
11 Abs. 1	Verbindliche unternehmensinterne Datenschutzvorschriften nach Artikel 16 Absatz 2 Buchstabe e DSG gelten für alle Unternehmen, die zum selben Konzern gehören.		Private	
11 Abs. 2	Sie umfassen mindestens die in Artikel 9 Absatz 1 genannten Punkte sowie die folgenden Angaben:	Vgl. die obenstehenden Kommentare zu Art. 9 E-VDSG.	Private	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	a. die Organisation und die Kontaktdaten des Konzerns und seiner Unternehmen; b. die innerhalb des Konzerns getroffenen Massnahmen zur Gewährleistung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften.	Die Regelung geht weniger weit als Art. 47 DSGVO. In der Praxis wird es allerdings kaum je rein schweizerische BCR geben. Die bisherigen BCR wurden regelmässig so abgefasst, dass sie auch EU-konform waren. Der EU-Standard muss auch nach revDSG genügen.		
12 Abs. 1	Personendaten dürfen ins Ausland bekannt gegeben werden, wenn durch einen Verhaltenskodex oder eine Zertifizierung ein geeigneter Datenschutz gewährleistet wird.			
12 Abs. 2	Der Verhaltenskodex enthält mindestens die Angaben nach Artikel 9 Absatz 1 und muss vorgängig vom EDÖB genehmigt werden.	Dies wird nicht möglich sein, da der Verhaltenskodex naturgemäss abstrakt und nicht für spezifische Unternehmen formuliert ist. Er wird somit beispielsweise die «Empfänger» (nicht: «Kategorien von Empfängern») nicht nennen. Dies ist jedoch gemäss dieser Bestimmung erforderlich. Ferner sollte nicht von «Angaben» die Rede sein, sondern von «Regelungen» oder «Punkten».	Private Bundesorgane	Der Verhaltenskodex «muss mindestens jene Punkte regeln, die nach dem Sinn und Zweck von Art. 9 Absatz 1 zu Regeln sind.»
12 Abs. 3	Der Verhaltenskodex oder die Zertifizierung muss mit einer verbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden.		Private Bundesorgane	
13 Abs. 1	Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit.	Art. 13 Abs. 1 E-VDSG verweist auf eine Informationspflicht des Auftragsbearbeiters, was im Erläuterungsbericht auch nochmals ausdrücklich betont wird. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor, diese besteht gemäss Art. 19 revDSG (korrekterweise) nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden. Art. 19 revDSG 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. Es sollte durch die Wortwahl «mitteilen» keine Verschärfung impliziert werden.	Private Bundesorgane	Die Erwähnung des Auftragsbearbeiters ist zu streichen. Es fehlt die gesetzliche Grundlage. Seine Erwähnung macht auch keinen Sinn. Es sollte nicht das Wort «mitteilen» verwendet werden, da es dafür keine gesetzliche Grundlage gibt. Korrekt wäre «Der Verantwortliche stellt die Information über die Beschaffung von Personendaten in präziser, verständlicher und

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Stattdessen sollte analog zu den Informationspflichten im Finanzmarktrecht der Begriff «zur Verfügung stellen» verwendet werden. Das bringt auch besser zum Ausdruck, dass die Information ein Betroffenenrecht darstellt, dessen Ausübung eine gewisse Mitwirkung des Betroffenen verlangt. Die Erläuterungen erwähnen, dass eine Kommunikation über eine Website nicht immer genügt. Die Person müsse wissen, dass sie die Informationen auf einer bestimmten Website findet, und es wird z.B. für Telefongespräche nahegelegt, dass ihr der Link mündlich mitgeteilt wird. Solche Ausführungen sind praxisfremd. Es sollte stattdessen festgehalten werden, dass die Information auf der Website genügt. Das entspricht der heutigen Praxis. Alles andere ist praxisfremd. Auch die Ausführungen in den Erläuterungen, wonach die betroffene Person die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhalten muss, ist schlicht falsch. Es gibt hierfür keine gesetzliche Grundlage, und es lässt jede Selbstverantwortung ausser Acht. Das ist auch deshalb bedenklich, weil der betroffenen Personen im Datenschutz eine Schlüsselrolle zukommt und es kontraproduktiv ist, ihr jede Eigeninitiative abzunehmen.		leicht zugänglicher Form zur Verfügung.» Es sollte festgehalten werden, dass eine Information über eine Website in der Regel genügt.
13 Abs. 2	Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.	Werden Piktogramme verwendet, müssen diese maschinenlesbar sein. Letzteres soll gemäss dem Erläuterungsbericht einen Vergleich verschiedener Dokumente und allgemein eine gewisse Automatisierung ermöglichen – es stellt sich die Frage, inwieweit dies ein Ziel des Datenschutzes ist. Die Pflicht unterliegt auch einem Überlegungsfehler. Die Piktogramme haben den Zweck, den Menschen einfacher als über Text anzusprechen und ihm zu ermöglichen, intuitiv auf eine Datenschutzerklärung zu reagieren. Soll dagegen eine automatisierte Auswertung einer Datenschutzerklärung erfolgen, müsste die Datenschutzerklärung selbst, nicht die Piktogramme maschinenlesbar bzw. ihre Inhalte entsprechend codiert sein, und zwar unabhängig davon, wie sie optisch dargestellt ist. Bei der Maschinelesbarkeit geht es ja gerade *nicht* um die optische Darstellung.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. Die Regel macht auch keinen Sinn und führt im schlimmsten Fall zur Strafbarkeit. Dies kann wiederum dazu führen, dass keine Piktogramme verwendet werden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Abgesehen davon gibt es für eine solche Pflicht keine gesetzliche Grundlage. Die Verwendung von Piktogrammen ist freiwillig, und daher darf der Verwender auch entscheiden, ob sie maschinenlesbar sind oder nicht, was auch immer dies bedeutet. Schliesslich fehlt es auch an Standards für solche Angaben. Ohne Standards macht eine solche Regel keinen Sinn.		
14	Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin.	Dies betrifft insbesondere die Statistik und Forschung. Die Regelung ist jedoch praxisfremd, denn es kann auch aus den Umständen hervorgehen, dass eine Auskunft freiwillig ist (Beispiel: Kundenzufriedenheitsumfrage eines Krankenversicherers)	Bundesorgane	Ergänzen mit «soweit dies nicht aus den Umständen ersichtlich ist»
15	Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.	Für diese «Informationspflicht bei der Bekanntgabe von Personendaten» gibt es keine gesetzliche Grundlage. Sie ist auch nach EU-Recht, auf welches sich der Erläuterungsbericht beruft, für private Datenbearbeiter nicht vorgeschrieben. Gegenüber der bisherigen Regelung in der VDSG wird die Vollständigkeit neu hinzugefügt, d.h. die Daten dürfen nicht lückenhaft sein. Die Regelung ist praxisfremd. Sie lässt sich nicht vernünftig umsetzen. Soll fortan jede E-Mail an eine andere Organisation einen entsprechenden Hinweis enthalten? Dazu kommt, dass der Empfänger ohnehin selbst verpflichtet ist, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern. Eine Information durch die übermittelnde Person unterläuft dies bzw. verabsolutiert eine der möglichen Vergewisserungsmassnahmen. Dies widerspricht dem Gesetz. Hinzu kommt, dass ein Auftragsbearbeiter etwas bekanntgeben soll, das er womöglich gar nicht hat.	Private Bundesorgane	Streichen, jedenfalls für private Datenbearbeiter. Es gibt keine gesetzliche Grundlage. Swiss Finish. Sie ist in dieser Form nicht praktikabel.
16	Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die	Die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, war bereits im Entwurf des revDSG vorgesehen und	Private Bundesorgane	Streichen. Es gibt keine gesetzliche Grundlage.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.	wurde vom Parlament gestrichen. Die Einführung dieser Pflicht über die revidierte Verordnung würde daher dem Willen des Parlaments widersprechen. Dieselbe Bestimmung verweist zudem auf ein Recht auf Einschränkung der Bearbeitung von Personendaten, das so im revDSG nicht besteht. Die Regelung erwähnt zudem die «Einschränkung» der Bearbeitung. Dies spielt auf Art. 18 DSGVO an, welche Bestimmung in der Schweiz so nicht existiert.		
17	Verlangt eine von einer automatisierten Einzelentscheidung betroffene Person, dass sie ihren Standpunkt darlegen kann oder dass eine natürliche Person die Entscheidung überprüft, so darf sie deswegen nicht benachteiligt werden.	Darin sind auch administrative Erschwernisse enthalten. Die Bestimmung bietet Potenzial für missbräuchliche Klagen gegen Verantwortliche, da diese auch nach einer Überprüfung einen Entscheid nicht anders fällen müssen. Es kann ihnen dann aber vorgeworfen werden, sie würden das nur deshalb nicht tun, weil um eine Überprüfung gebeten wurde.	Private Bundesorgane	
18	Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.	Schriftlich ist an dieser Stelle mit Papierform oder elektronischer Form gemeint. Der Begriff ist nicht als handschriftlich zu verstehen. Für eine solche Aufbewahrungspflicht gibt es keine gesetzliche Grundlage. Im revDSG wurde bewusst auf solche Dokumentationspflichten verzichtet, abgesehen vom Verzeichnis. Die Regelung geht ferner davon aus, dass eine Datenschutz-Folgenabschätzung nie erneuert wird. Dies entspricht jedoch nicht der Praxis. Es ist nicht klar, wie mit mehreren Datenschutz-Folgenabschätzungen umzugehen ist.	Private / Bundesorgane	Klarstellen: «… muss in der aktuellsten Fassung während zwei Jahren …» Die Aufbewahrungspflicht ist zu streichen. Es fehlt eine gesetzliche Grundlage. So oder so ist sie als Mindestfrist auszugestalten. Es ist klarzustellen, dass Schriftlich «in Textform» meint.
19 Abs. 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;	Art. 19 stellt eine Präzisierung von Art. 24 revDSG dar und ist so zu verstehen, dass im Falle einer Meldung an den EDÖB diese die in Art. 19 Abs. 1 VDSG aufgeführten Punkte enthalten muss. Die Einschränkung «soweit möglich» macht Sinn, da die Angabe in der Praxis oft nicht möglich ist. Bst. a und b gehen über die DSGVO hinaus, doch dürfte dies in der Praxis kein Problem darstellen.	Private Bundesorgane	Im Einleitungssatz ist aufzunehmen: «… bei einer meldepflichtigen Verletzung …» Bst. e ist umzuformulieren: «die Folgen für die betroffenen Personen, von welchen ein hohes Risiko ausgeht» Es sollte eine «de minimis»-Regelung vorgesehen werden, in welchen trotz eines hohen

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern; g. den Namen und die Kontaktdaten einer Ansprechperson.	Falsch formuliert ist hingegen Bst. e. 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 Bst. 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). Gemäss den Erläuterungen wird das in Art. 24 Abs. 2 revDSG erwähnte «voraussichtlich» so interpretiert, dass auch dann gemeldet werden muss, wenn das Vorliegen eines «hohen Risikos» nicht ausgeschlossen werden kann. Diese Aussage hilft nicht weiter, da es sich um einen Pleonasmus handelt. Der Begriff «Risiko» beinhaltet bereits eine Wahrscheinlichkeitsüberlegung, d.h. wie wahrscheinlich es ist, dass ein Schaden eintritt. Es bleibt dabei: Die Wahrscheinlichkeit muss eine gewisse Höhe aufweisen.Wünschenswert wäre schliesslich eine «de minimis»-Regelung, die jene Fälle ausschliesst, in welchen der EDÖB ohnehin nicht wirklich etwas tun kann oder will, obwohl ein hohes Risiko vorliegt (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, die er für andere, für den Datenschutz wichtigere Angelegenheiten einsetzen kann.		Risikos für eine betroffene Person nicht gemeldet werden muss. Bst. f. sollte angepasst werden: "gegebenenfalls welche Massnahmen getroffen wurden …"
19 Abs. 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.	Der Hinweis «bei Entdeckung der Verletzung der Datensicherheit» erscheint wenig sinnvoll. Zu diesem Zeitpunkt wird der Verantwortliche nie über alle Informationen verfügen, da sich diese immer erst über Zeit herausstellen. Der Hinweis kann ersatzlos gestrichen werden.		Streichung von «bei Entdeckung der Verletzung der Datensicherheit»
19 Abs. 3	Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mit.	Gemäss Art. 24 rev DSG enthält die Meldung an den EDÖB mind. die Art der Verletzung der Datensicherheit, Folgen, ergriffene und vorgesehene Massnahmen. Die Angaben, die an die Betroffenen gemacht werden müssen sind: die Art der Verletzung, die Folgen und Risiken, die Massnahmen sowie Name		

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		und Kontaktdaten der Ansprechperson. Es sind also fast dieselben Vorgaben, wie an den EDÖB, diese sind jedoch sprachlich einfacher zu halten.		
19 Abs. 4	Handelt es sich beim Verantwortlichen um ein Bundesorgan, so erfolgt die Meldung an den EDÖB über die Datenschutzberaterin oder den Datenschutzberater.	Mittels Weisung o.Ä. muss sichergestellt werden, dass in einem Fall einer Datensicherheitsverletzung die gemeldet werden muss, der DSB sofort informiert wird.	Bundesorgane	
19 Abs. 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.	Eine Dokumentationspflicht kennt zwar die DSGVO. Das revDSG sieht sie jedoch nicht vor. Daher kann sie und die entsprechende Aufbewahrungspflicht auch nicht auf dem Weg der Verordnung eingeführt werden. Noch die Botschaft zum revDSG hielt fest, dass keine allgemeine Dokumentationspflicht eingeführt werden soll. Genau dies wird hier (und in anderen Bestimmungen) durch die Hintertür versucht. Es bleibt jedenfalls unklar, wozu die Dokumentations- und Aufbewahrungspflicht dient, ausser allenfalls dem EDÖB. Da sich aus der Systematik aber ergibt, dass ohnehin nur meldepflichtige Verletzungen zu dokumentieren sind, erschliesst sich auch dieser Sinn nicht wirklich: Ist gemeldet und interessiert sich der EDÖB dafür, wird er sofort nachfragen. Tut er dies nicht, wird er kaum später darauf zurückkommen. Der Hinweis auf alle «zusammenhängenden Tatsachen» ist falsch, denn er suggeriert, dass Tatsachen nur für die Dokumentationspflicht erforscht werden müssen, was sicherlich nicht erforderlich ist. Warum hier drei statt wie sonst zwei Jahre vorgesehen sind, ist unklar.	Private Bundesorgane	Streichen. Es fehlt die gesetzliche Grundlage. Die Norm ist auch nicht nötig. Der Begriff «Tatsachen» ist durch «und dokumentierten Tatsachen» zu präzisieren.
20 Abs. 1	Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden.	Mit schriftlich ist hier auch die elektronische Form gemeint. Zu beachten ist, dass der Verantwortliche auf mündliche Begehren nicht reagieren muss. Die Bestimmung erscheint daher wenig sinnvoll.	Private Bundesorgane	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
20 Abs. 2	Die Auskunft wird in der Regel schriftlich erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat.	Auch hier meint schriftlich entweder auf Papier oder elektronisch.	Private Bundesorgane	
20 Abs. 3	Die Auskunft muss für die betroffene Person verständlich sein.	Sie muss verständlich sein. Ob die betroffene Person sie im konkreten Fall versteht, ist nicht relevant. Beim Auskunftsbegehren geht es darum, die bearbeiteten Daten mitzuteilen. Müssen diese noch so erläutert werden, dass sie für die betroffene Person verständlich sind, kann dies zu einem unverhältnismässigen Aufwand führen. Das Auskunftsrecht bietet Zugang zu Daten, nicht ein Recht darauf, die Datenbearbeitung so lange erklärt zu bekommen, bis sie die jeweilige Person versteht. Eine solche Pflicht hat keine Grundlage im Gesetz. 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, sind aufwändige Erläuterungen erforderlich, mitunter auch sehr viel Fachwissen. Abgesehen davon, dass dies nicht unbedingt innerhalb von 30 Tagen erfolgen kann, sprengt dies jeden Rahmen und ist unverhältnismässig. Nirgends in Europa wird das Auskunftsrecht so verstanden.	Private Bundesorgane	Den Begriff «für die betroffene Person» streichen. Statt «verständlich» soll «im Grundsatz nachvollziehbar sein, sofern damit kein unverhältnismässiger Aufwand verbunden ist» verwendet werden. Eine Alternative wäre folgende Formulierung: «Die Auskunft darf nicht irreführend sein.»
20 Abs. 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.	Es fehlt eine gesetzliche Grundlage für eine echte Verpflichtung der betroffenen Person. Insofern macht Satz 2 wenig Sinn. Lässt sich die Identität der betroffenen Person nicht verifizieren, erhält sie auch keine Auskunft.	Private Bundesorgane	Begriff «Identifizierung» ersetzen durch den Begriff «Authentifizierung»
20 Abs. 5	Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Auf-	Diese Dokumentation kann bspw. durch eine Kopie des Antwortschreibens erreicht werden. Bei einer mündlichen Auskunft müsste daher z.B. eine Telefonnotiz erstellt werden.	Private Bundesorgane	Streichen. Es fehlt eine gesetzliche Grundlage. Die Bestimmung bietet keinen Mehrwert,

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	schub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.	Das revDSG sieht keine solche Dokumentations- und Aufbewahrungspflicht vor. Sie kann nicht auf dem Verordnungsweg eingeführt werden. Sie ist auch wenig sinnvoll. Sie zwingt den Verantwortlichen, Personendaten entsprechend länger aufzubewahren bzw. mehr Personendaten zu beantworten, als er dies womöglich tun würde. Die betroffene Person erhält eine Antwort auf ihr Ersuchen. Will sie dagegen vorgehen, kann sie diese Antwort ins Recht legen. Die Bestimmung sorgt nur für zusätzlichen Aufwand. Wie sich die drei Jahre herleiten, ist unklar.		sorgt aber für zusätzlichen Aufwand.
21 Abs. 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.	Das DSG nimmt auf den Begriff der gemeinsamen Verantwortlichen sonst normalerweise keinen Bezug. Die Regelung ist jedoch konsequent. Unklar ist, welche Rechtsfolge die «Unzuständigkeit» eines Verantwortlich hat.	Private Bundesorgane	Es ist zu präzisieren: "Sind für die Bearbeitung von Personendaten mehrere gemeinsam verantwortlich …"
21 Abs. 2	Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.	Diese Bestimmung ist verwirrlich, da sie 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. Die Regelung sollte präzisiert werden.	Private Bundesorgane	Am Ende sollte es heissen: «sofern er das Begehren nicht im Auftrag des Verantwortlichen selbst beantwortet.»
22 Abs. 1	Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen.	Die Frist kann erst dann zu laufen beginnen, wenn das Begehren klar und die betroffene Person korrekt identifiziert ist. Dies ist sie zu Beginn häufig nicht.	Private Bundesorgane	Zu präzisieren: «… seit dem Vorliegen eines klaren Begehrens und der korrekten Identifikation der betroffenen Person.»
22 Abs. 2	Kann die Auskunft nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr die Frist mitteilen, in der die Auskunft erfolgen wird.		Private Bundesorgane	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
23 Abs. 1	Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist.	Es ist nicht von einem unverhältnismässigen Aufwand zu sprechen, wenn der Verantwortliche nicht genügend Strukturen im Unternehmen hat, was zu grossem Arbeitsaufwand führt (wobei damit Fälle der Missachtung des Grundsatzes des «Privacy by Design» gemeint sind).	Private Bundesorgane	
23 Abs. 2	Die Beteiligung beträgt maximal 300 Franken.	Der Betrag wird nicht verändert, weil es seit seiner Einführung zu keiner relevanten Teuerung gekommen sei und der Betrag nicht abschreckend sein soll. Allerdings steht dieser Kostendeckel im Vergleich zum Aufwand, den ein Auskunftsersuchen trotz entsprechender Strukturen mit sich bringen kann, in keinem Verhältnis (z.B. können umfassende Schwärzungen erforderlich sein, was Kosten pro Fall von CHF 10'000 mit sich bringen kann). Auch die DSGVO kennt keine betragsmässige Begrenzung, sondern verlangt, dass er «angemessen» ist. Auch im Öffentlichkeitsrecht kann eine Gebühr verlangt werden. Der Betrag soll durchaus abschreckend sein, weil er die betroffenen Personen dahingehend diszipliniert, Auskunftsersuchen nur dann zu stellen, wenn sie wirklich angezeigt sind und nicht aus Jux.	Private Bundesorgane	Betrag den Verhältnissen anpassen (mindestens CHF 3'000) Alternativ ist die Bestimmung zu streichen, da die angemessene Kostenbeteiligung bereits in Abs. 1 enthalten ist. Beispiel: Aufwand bis CHF 500 trägt das Unternehmen, darüber hinaus müssen die Kosten zu 50% übernommen werden.
23 Abs. 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.	Es ist zu präzisieren, dass die Antwortfrist von 30 Tagen erst danach beginnt.	Private Bundesorgane	Präzisieren: «Erst danach beginnt die Frist zur Beantwortung des Auskunftsbegehrens.»
24	Die Artikel 20 Absätze 1, 4 und 5, sowie 21, 22 und 23 sind auf das Recht auf Datenherausgabe und -übertragung sowie deren Einschränkungen sinngemäss anwendbar.		Private Bundesorgane	
25	Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrektur-	Es ist schon konzeptionell nicht richtig, dass der Datenschutzberater die Aufgaben «wahrnehmen» muss, er muss sie «haben». Zu lit. a: Die breite der Prüfpflicht geht am Ziel vorbei, als sie impliziert, dass der Datenschutzberater im Grund kein Berater mehr ist, sondern als "Datenschutzpolizist" agieren sollte, d.h.	Private	Die Bestimmung sollte gestrichen werden, da im Gesetz bereits alles nötig gesagt wird. Sie stammt noch aus einer Zeit, in welcher das Gesetz

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	massnahmen, wenn sie oder er feststellt, dass 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.	alles und jeden in Bezug auf den Datenschutz zu überprüfen. Richtig wäre stattdessen, dass seine beratende Funktion betont wird, und zwar dort, wo ihn die verantwortlichen Stellen beiziehen wollen. Das ist auch das Prinzip, das der Gesetzgeber bei der DSFA verfolgt: Wenn der Verantwortliche die DSFA nicht dem EDÖB vorlegen will, was er kann, dann kann er sie stattdessen dem Berater vorlegen. So sieht es auch Art. 10 Abs. 2 Bst. a revDSG vor. Dem ist hier Rechnung zu tragen. Der Berater sollte nur auf Beizug aktiv werden. Abgesehen davon ist beim bestehenden Vorschlag unklar, in welchem Umfang die Bearbeitungen zu prüfen sind (alle, einige, nur die ihm vorgelegten, nur nach Risiko) und welche Folgen es hat, wenn der Datenschutzberater dieser Aufgabe nicht nachkommt. Die Erläuterungen implizieren, dass alle Bearbeitungsaktivitäten überprüft werden müssen, was nicht richtig sein kann. Auch hier kann risikoorientiert geprüft werden. Mit den «Voraussetzungen» sind die internen Datenschutzvorschriften gemeint, die der Datenschutzberater ebenfalls überprüfen soll. Die Erläuterungen implizieren daher, dass der Datenschutzberater eine andere Stelle sein soll als die interne Datenschutzstelle, welche solche Vorschriften ausarbeitet. Dies ist dem Konzept des Datenschutzbeauftragten der DSGVO angelehnt. Die Erläuterungen betonen auch, dass der Datenschutzberater für die Datenbearbeitung nicht verantwortlich ist. Zu lit. b: Nur das Vorlegen der DSFA dem/der DSB genügt nicht, der/die DBS muss bei der Erstellung der DSFA mitwirken. Dabei müssen die Risikobewertung und vorgeschlagenen Massnahmen geprüft werden.		noch keine solchen Ausführungen enthielt. Wird sie beibehalten, ist sie zu präzisieren: «Der Datenschutzberaterin oder dem Datenschutzberater eines privaten Verantwortlichen müssen folgende Aufgaben übertragen worden sein:» Bst. a ist anzupassen: "Wo sie oder er beigezogen wird, prüft sie oder er die Bearbeitung …"
25 Abs. 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		Private	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	zur Erfüllung ihrer oder seiner Aufgaben benötigt.			
26	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.	Unternehmen mit weniger als 250 Mitarbeitenden (wohl nicht FTE) müssen folglich nur diejenigen Bearbeitungstätigkeiten in Verzeichnissen dokumentieren, die die genannten Kriterien erfüllen, d.h. eine Datenbearbeitung durchführen, die ein hohes Risiko mit sich bringt. Unklar ist, ab wann «umfangreich» besonders schützenswerte Personendaten bearbeitet werden. Genügt die Bearbeitung von HR-Daten? Sind die Voraussetzungen für die Befreiung nicht erfüllt, ist das Verzeichnis für alle Bearbeitungsaktivitäten zu führen. Dies impliziert jedenfalls der Wortlaut der Bestimmung. Art. 12 Abs. 5 revDSG erlaubt die Ausnahme nur, wenn ein «geringes Risiko» vorliegt. Demnach ist der Bundesrat der Auffassung, dass wenn weder Bst. a noch b erfüllt ist, per se ein geringes Risiko vorliegt. Das würde den Anwendungsbereich von Art. 22 revDSG (DSFA) stark einschränken. Zudem ist darauf hinzuweisen, dass diese Ausnahme bei Art. 3 und 4 nicht vorgesehen ist, was zu absurden Folgen führt. Generell sollten für Verzeichnisse Übergangsfristen vorgesehen werden, da sie einen sehr hohen Aufwand mit sich bringen.	Private	Es ist klarzustellen, dass wenn eine der beiden Voraussetzungen erfüllt ist, die Verzeichnispflicht nur für die entsprechenden Bearbeitungen mit hohem Risiko gelten. Der Begriff der Mitarbeitenden ist durch "Vollzeitstellen" zu ersetzen. Es ist eine Übergangsfrist zur Umsetzung der Verzeichnispflicht von einem Jahr vorzusehen.
27	Jedes Bundesorgan ernennt eine Datenschutzberaterin oder einen Datenschutzberater. Mehrere Bundesorgane können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen.		Bundesorgan	
28 Abs. 1	Die Datenschutzberaterin oder der Datenschutzberater muss die folgenden Anforderungen erfüllen: a. Sie oder er verfügt über die erforderlichen Fachkenntnisse.	Für die Privaten wurde dies im revDSG bereits aufgeführt. Für die Bundesorgane wird es jetzt auf Verordnungsstufe ebenfalls noch eingeführt.	Bundesorgane	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	b. Sie oder er übt ihre oder seine Funktion gegenüber dem Bundesorgan fachlich unabhängig und weisungsungebunden aus.			
28 Abs. 2	Sie oder er muss folgende Aufgaben wahrnehmen: a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden. b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese. c. Sie oder er meldet dem EDÖB Verletzungen der Datensicherheit. d. Sie oder er dient als Anlaufstelle für die betroffenen Personen. f. Sie oder er schult und berät das Bundesorgan sowie dessen Mitarbeiterinnen und Mitarbeiter in Fragen des Datenschutzes.		Bundesorgane	
29 Abs. 1	Das Bundesorgan gewährt der Datenschutzberaterin oder dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.		Bundesorgane	
29 Abs. 2	Es veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutz-beraters im Internet und teilt diese dem EDÖB mit.	Der Name des DSB ist nicht zwingend anzugeben, es genügt, eine E-Mail-Adresse der zuständigen Stelle.	Bundesorgane	
30	Die Datenschutzberaterin oder der Datenschutzberater dient dem EDÖB als Anlaufstelle für Fragen im Zusammenhang mit der Bearbeitung von Personendaten durch das betreffende Bundesorgan.		Bundesorgane	

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
31	Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.	Es ist unklar, was «sogleich» bedeuten soll. Es muss genügen, dass die Erfordernisse des Datenschutzes im Projekt rechtzeitig berücksichtigt werden.	Bundesorgane	Der Begriff «sogleich» ist durch «rechtzeitig» zu ersetzen.
32 Abs. 1	Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.	Bereits geplante automatisierte Bearbeitungstätigkeiten müssen gemeldet werden, was zu einem erheblichen Mehraufwand für die Dokumentation führt. Zudem muss jede geplante automatisierte Bearbeitung gemeldet werden, nicht nur solche mit einem (potenziellen) hohen Risiko. Die Meldung muss im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung erfolgen. Diese erfolgen oft auf der Basis eines vorgegebenen Rahmens, während die konkreten Entscheidungen erst im Verlauf des Projekts getroffen werden. Daraus folgt, dass die verlangten Angaben in dem Zeitpunkt in der Regel noch nicht in der genügenden Detailtiefe vorliegen werden. Zudem sollte sich gemäss Botschaft zu Art. 11 Abs. 4 E-DSG (Art. 12 Abs. 4 revDSG) keine Änderung im Vergleich zum bestehenden Recht ergeben. Eine Pflicht, geplante Datensammlungen dem EDÖB zu melden, besteht aber nach geltendem Recht nicht. Es fehlt daher an einer gesetzlichen Grundlage. Gemäss Erläuterungsbericht dient die frühe Meldung zudem nicht dem Persönlichkeitsschutz, sondern der Ressourcenplanung des EDÖB. Art. 47 E-VDSG enthält eine Übergansbestimmung für automatisierte Bearbeitungstätigkeiten, die bei Inkrafttreten des E-VDSG bereits produktiv sind.	Bundesorgane	Streichen, es fehlt die gesetzliche Grundlage. Zudem liegen die zu meldenden Informationen im Zeitpunkt, in dem die Meldung erfolgen soll, in der Regel nicht in der genügenden Detailtiefe vor. Die Ressourcenplanung des EDÖB rechtfertigt zudem nicht den mit dieser frühen Meldung einhergehenden Mehraufwand der Bundesbehörden.

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
		Diese Übergangsbestimmung ist insofern keine Erleichterung, als für bereits produktive Bearbeitungen ein Verzeichnis erstellt und dieses an den EDÖB gemeldet werden muss.		
32 Abs. 2	Die Meldung muss die Angaben nach Artikel 12 Absatz 2 Buchstaben a-d DSG sowie das voraussichtliche Datum des Beginns der Bearbeitungstätigkeiten enthalten.	Es muss somit ein «vorsorgliches Verzeichnis» gemeldet werden.	Bundesorgane	
32 Abs. 3	Das verantwortliche Bundesorgan aktualisiert die Meldung beim Übergang in den produktiven Betrieb oder bei der Projekteinstellung.		Bundesorgan	
33	Eine Testphase als Pilotversuch ist unentbehrlich, wenn eine der folgenden Bedingungen erfüllt ist: a. Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen. b. Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone. c. Die Erfüllung der Aufgaben erfordert, dass die Personendaten mittels eines Abrufverfahrens zugänglich gemacht werden.			
34 Abs. 1	Vor der Konsultation der interessierten Verwaltungseinheiten legt das für den Pilotversuch zuständige Bundesorgan zu Handen des EDÖB dar, wie die Einhaltung der Anforderungen nach Artikel 35 DSG gewährleistet werden soll, und lädt ihn zur Stellungnahme ein.			
34 Abs. 2	Der EDÖB nimmt zur Frage Stellung, ob die Bewilligungsvoraussetzungen nach Artikel 35 DSG erfüllt sind. Das zuständige Bundesorgan stellt ihm alle dazu not-wendigen Unterlagen zur Verfügung, insbesondere:			

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	a. eine allgemeine Beschreibung des Pilotversuchs; b. einen Bericht, der nachweist, dass die Erfüllung der gesetzlich vorgesehenen Aufgaben die Bearbeitung im Sinne von Artikel 34 Absatz 2 DSG erfordert und dass eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn unentbehrlich ist (Artikel 35 Absatz 1 Buchstabe c DSG); c. eine Beschreibung der internen Organisation sowie der Datenbearbeitungs- und Kontrollverfahren; d. eine Beschreibung der Sicherheits- und Datenschutzmassnahmen; e. den Entwurf einer Verordnung, welche die Einzelheiten der Bearbeitung regelt, oder das Konzept einer Verordnung; f. die Informationen betreffend die Planung der verschiedenen Phasen des Pilotversuches.			
34 Abs. 3	Der EDÖB kann weitere Dokumente anfordern und zusätzliche Abklärungen vornehmen.			
34 Abs. 4	Das zuständige Bundesorgan informiert den EDÖB über jede wichtige Änderung, welche die Einhaltung der Anforderungen von Artikel 35 DSG betrifft. Der EDÖB nimmt, falls erforderlich, erneut Stellung.			
34 Abs. 5	Die Stellungnahme des EDÖB ist dem Antrag an den Bundesrat beizufügen.			
34 Abs. 6	Die Modalitäten der automatisierten Datenbearbeitung werden in einer Verordnung geregelt.			
35	Das zuständige Bundesorgan legt dem EDÖB den Entwurf des Evaluationsberichts an den			

Artikel	Text	Bemerkungen	Private / Bundesorgan	Anpassungsvorschlag
	Bundesrat zur Stellungnahme vor. Die Stellungnahme des EDÖB ist dem Bundesrat zur Kenntnis zu bringen.			
36	Werden Personendaten zu nicht personenbezogenen Zwecken, insbesondere Forschung, Planung und Statistik, und gleichzeitig zu einem anderen Zweck bearbeitet, so sind die Ausnahmen nach Artikel 39 Absatz 2 DSG nur für die Bearbeitung zu den nicht personenbezogenen Zwecken anwendbar.			
45 Abs. 1	Die vom EDÖB in Rechnung gestellten Gebühren bemessen sich nach dem Zeitaufwand.			
45 Abs. 2	Es gilt ein Stundenansatz von 150 bis 350 Franken. Dieser richtet sich nach der Komplexität des Geschäfts und nach der Funktion der für die Bearbeitung zuständigen Person.			
45 Abs. 3	Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004.			
47	Artikel 32 ist nicht anwendbar auf geplante automatisierte Bearbeitungstätigkeiten, bei welchen im Zeitpunkt des Inkrafttretens die Projektfreigabe oder der Entscheid zur Projektentwicklung bereits erfolgt ist.			

Autoren: Maria Winkler (Basisdokument, Kommentierung), David Rosenthal (Kommentierung, Anpassungsvorschläge), David Vasella (Anpassungsvorschläge). Berücksichtigt wurde auch die Kommentierung von David Vasella (https://datenrecht.ch/zum-entwurf-der-revidierten-vdsg-eine-verpasste-chance/ und https://datenrecht.ch/taeglich-gruesst-das-murmeltier-gedanken-zum-vorentwurf-der-datenschutzverordnung/). Ferner wurden die Bemerkungen und Kommentare der Mitglieder des VUD anlässlich der Fachsitzung vom 1. September 2021 verarbeitet.