Datenschutz Forum Schweiz

Zürich, 12. Oktober 2021

Bundesamt für Justiz
Direktionsbereich Öffentliches Recht
Bundesrain 20
3003 Bern

Vernehmlassung zur Totalrevision der

Verordnung zum BG über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Datenschutz-Forum Schweiz wurde im September 1999 als Verein mit dem Zweck gegründet, die praktische Umsetzung sowie die Forschung auf dem Gebiet des Datenschutzes und der Datensicherheit zu fördern. Seit nunmehr 22 Jahren geschieht dies insbesondere durch den Informations- und Erfahrungsaustausch unter den am Datenschutz interessierten Personen aus allen Fachrichtungen der Wirtschaft, der öffentlichen Verwaltung und der Wissenschaft.

Für betroffene Personen, Datenbearbeitenden, Behörden, Politiker und Medien stellt das Datenschutz-Forum Schweiz Informationen sowie Unterlagen für die Meinungs- und Entscheidungsfindung in Datenschutz- und Datensicherheitsfragen zur Verfügung. Es fördert die Aus- und Weiterbildung auf diesem Gebiet und pflegt Kontakte zu Organisationen mit gleichen Zielsetzungen.

Vor diesem Hintergrund nehmen wir gerne die Gelegenheit wahr, uns am Vernehmlassungsverfahren zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz zu beteiligen und dazu Stellung zu nehmen. Das Datenschutz-Forum Schweiz hat sich bei seinen Bemerkungen v.a. auf Grundlegendes im Vorentwurf beschränkt oder sich auf Normen konzentriert, welche erheblich nachbesserungsfähig sind. Die Vorlage hat insgesamt gelungene Vorschläge wie eine bessere Systematik, insgesamt erscheint sie aber leider noch zu unausgereift und zahlreiche Bestimmungen sind losgelöst von den gesetzlichen Grundlagen im nDSG und auch von der DSGVO. Aus Kapazitätsgründen konnten wir diese nicht alle in unserer Vernehmlassung thematisierten.

1. Allgemeines

Die Verordnungsartikel sind vom Wortlaut her häufig aus sich heraus nicht gut verständlich, sondern benötigen den „Erläuternden Bericht zur Revision der Verordnung zum BG über den Datenschutz". Dies ist insofern bedauerlich, da damit zu rechnen ist, dass Verantwortliche von personenbezogenen Datenbearbeitungen sich lediglich am Gesetzes- und Verordnungstext orientieren. Deshalb schlagen wir generell vor, dass der Verordnungstext sprachlich präziser gestaltet wird, dabei teilweise auch mit Beispielen zur besseren Verständlichkeit gearbeitet wird oder auch nochmals Bezug auf den Gesetzestext genommen wird. Wir vermissen im Entwurf die durchgehende Berücksichtigung des Leitfadens zur geschlechterneutralen Formulierung:
(s.https://www.bk.admin.ch/bk/de/home/dokumentation/sprachen/hilfsmittel-textredaktion/leitfaden-zum-geschlechtergerechten-formulieren.html).
Wir würden es begrüssen, wenn bei den «einleitenden» Allgemeinen Bestimmungen die Verantwortlichen und Auftragsbearbeitenden als Hauptadressaten der meisten Normen häufiger genannt werden würden, damit sich diese ihrer umfangreichen Verantwortung bewusst sind.

2. Stellungnahmen zu einzelnen Normen

Art. 1 E-VDSG (Grundsätze) Für Art. 1 E-VDSG wurde Art. 8 Abs. 1 nDSG übernommen, aber durch eine geänderte Satzstellungen und Hinzufügungen hat die Norm in ihrer Aussagekraft bzw. in ihrer Verständlichkeit gelitten. Hier schlagen wir vor, Verantwortliche und Auftragsbearbeitende wieder namentlich aufzuführen (vgl. unsere Bemerkungen unter «1. Allgemeines»). Unser Vorschlag wäre, Art. 8 Abs. 1 nDSG als klar verständlichen Einleitungssatz zu übernehmen. Wir sind uns bewusst, dass eine Wiederholung des Textes auf Verordnungsebene in der Regel redaktionell unerwünscht ist. Aber wir betrachten eine Wiederholung eines klaren Gesetzestextes als weniger problematisch als eine Grundsatznorm, die mit dem Wort «Ob» beginnt.
Im zweiten Satz können dann die Kriterien folgen. Hier sollte das Wort «insbesondere» einfliessen, damit den Normadressaten klar wird, dass diese nicht vollständig aufgelistet sind. Es finden sich in Art. 8 Abs. 1 nDSG keine Hinweise darauf, dass der Gesetzgeber die Kriterien begrenzen wollte und eine solche Begrenzung ist u.E. auch nicht sinnvoll.

Dadurch kann auch auf den Begriff «Umstände» in Abs. 1 Bst. c E-VDSG verzichtet werden, da dieser als Ergänzung falsch gewählt worden ist, um künstliche Intelligenz als besonders hohes Risiko einer automatisierten Datenbearbeitung aufzuführen. Erstens ist er bereits in der «Art» der Datenbearbeitung erfasst, und zweitens entsteht der Eindruck, dass noch rasch der Entwurf der EU-Kommission für eine KI-Verordnung in der Vorlage berücksichtigt werden sollte. Es wäre aus unserer Sicht wün

schenswert, wenn die datenschutzrechtliche Auseinandersetzung mit der möglichen Normierung von KI-Technologien gründlicher erfolgt.

Unser Änderungsvorschlag:

Art. 1 Grundsätze

[1] Der Verantwortliche und der Auftragbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit. Dies beurteilt sich insbesondere nach den folgenden Kriterien:

a. Zweck, Art und Umfang der Datenbearbeitung;…

Art. 2 E-VDSG (Schutzziele): Als redaktionellen Vorschlag empfehlen wir Ihnen, den Einleitungssatz der Norm umzustellen: In seiner jetzigen Form kann der Sinn der Angemessenheit falsch verstanden werden. Wir weisen in diesem Zusammenhang auf den DSG-Kurzkommentar von Bruno Baeriswyl zu Art. 7 hin (S. 92 ff.).

Zudem ist eine abschliessende Auflistung von Schutzzielen nicht zielführend, da es sich bei der anschliessenden Auflistung nicht um Schutzziele handelt, sondern um technische und organisatorische Massnahmen, welche die Datensicherheit bei der Bearbeitung personenbezogener Daten beinhaltet. Hier ist für uns nicht nachvollziehbar, dass gemäss „Erläuterndem Bericht" grösstenteils Art. 9 VDSG übernommen wurde, der bereits seit Jahren als antiquiert gilt. Wir vertreten die Ansicht, dass die nicht abschliessend (vgl. unsere Bemerkung zu Art. 1 E-VDGS) aufgezählten Massnahmen, die zum angestrebten Schutzziel lenken, gemeinsam mit Informatik- und Datenschutzexpert:innen nochmals überprüft und bereinigt werden. Dabei wären auch die DSGVO und internationale Standards als Materialien beizuziehen. Wir schlagen bei diesen vor, auf absolute Verben wie «verunmöglichen» (Art. 2 Abs. 2 Bst. c) zu verzichten und eher Verben wie «sicherzustellen» einzusetzen.

Der Katalog der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden, womit die Liste auch mit Art. 32 DSGVO konform wäre.

Diese Massnahmen sind natürlich zu trennen von technischen und organisatorischen Bestimmungen, welche den Schutz der Rechtmässigkeit der Verarbeitung beinhalten (unterschiedlicher Gegenstand).

Unser Änderungsvorschlag:

Art. 2 Schutzziel

Die Verantwortlichen müssen dafür sorgen, dass alle notwendigen Massnahmen zur Datensicherheit getroffen werden, damit ein angemessener Schutz derjenigen Personen gewährleistet ist, deren Daten sie bearbeiten. Dazu zählen namentlich: .....

Art. 3 E-VDSG (Protokollierung): Der Begriff «private Verantwortliche» wird in Absatz 1 eingeführt. Dies irritiert, da diese Bezeichnung nicht in Art. 5 nDSG erklärt wird, und es somit an der notwendigen gesetzlichen Grundlage fehlt, weshalb alternativ überlegt werden muss, ob dieser Artikel allenfalls auch zu streichen ist. Zudem wird es in den wenigsten Betrieben die Aufgabe des «Verantwortlichen» sein, zu protokollieren. Vielmehr hat er (oder sie) dafür zu sorgen, dass protokolliert wird. Der Auftraggeber ist sowieso verpflichtet, zu protokollieren, falls dies zu den Pflichten des Verantwortlichen gehört.

Das Wort «zumindest» beinhaltet eine Wertung in der Norm, die jedoch keine Rechtsfolge auslöst, dementsprechend kann auf dieses Wort in den Absätzen 1 und 2 verzichtet werden.

Absatz 4: Hier fragen wir uns, ob der Ausdruck «für diesen Zweck» inhaltlich korrekt ist.

Unser Änderungsvorschlag:

Art. 3 Protokollierung *[1] …, sorgt der Verantwortliche einer privaten Person dafür, dass folgende Vorgänge protokolliert werden:…* *[4]* …, und dürfen nur im Rahmen dieser Aufgabenerfüllung bearbeitet werden *Alternativ: Artikel streichen*

Art. 4 E-VDSG (Bearbeitungsreglement von privaten Personen): Die Verknüpfungen von Datenbeständen gehören zu den grössten Risiken für die Datensicherheit im Betrieb. Dementsprechend sollte das Bearbeitungsreglement von privaten Personen auch solche Verknüpfungen aufführen. Auch hier fehlt es an der notwendigen Grundlage, und das Verhältnis zum Bearbeitungsverzeichnis (BV) ist unklar und redundant, weshalb alternativ diese Bestimmung auch gestrichen werden kann.

Art. 5 E-VDSG (Bearbeitungsreglement von Bundesorganen): Die Regelung ist einerseits unverhältnismässig, andererseits fehlt es an der entsprechenden gesetzlichen Grundlage, weshalb der Artikel zu streichen ist.

Art. 6 E-VDSG (Modalitäten): Sprachlicher Verbesserungsvorschlag:
Der Verantwortliche kann nicht sicherstellen, sondern lediglich für die vertrags- und gesetzesmässige Bearbeitung sorgen. Auch ist die Form der Zustimmung unklar formuliert.

Unser Änderungsvorschlag:

Art. 6 Modalitäten *[2] Untersteht der Auftragbearbeiter nicht dem DSG,… .... die Zustimmung erfolgt schriftlich oder in elektronischer Form.....*

Art. 7 E-VDSG (Informationen an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans): Art. 7 stützt sich auf Art. 9 nDSG ab. Hier hat der Bundesrat relativ viel Gestaltungsraum, wie Datenschutzberatende einzubeziehen sind. In der Praxis ist es wesentlich effektiver, wenn

Datenschutzberatende vorgängig in solche Projekte einbezogen werden. Dadurch kann das Fachwissen bereits bei der Projektplanung einbezogen werden, damit sie ihre Beratungsfunktion erfüllen können. Datenschutzbeauftragte sind sinnvollerweise vor allem präventiv aktiv und dies sollte bei der Ausgestaltung dieses Artikels unbedingt berücksichtigt werden, damit nachfolgende Probleme bei der Einhaltung von Datenschutzvorschriften soweit wie möglich vermieden werden können. Dies kann im Rahmen einer vorgängigen Konsultation der datenschutzbeauftragten Person geschehen, wobei auch der Einsitz in entsprechende Gremien dazu zählt. Hier verweisen wir auch auf die Leitgedanken zur Revision des DSG (vgl. u.a. 17.059 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, S. 6943).

Art. 9 E-VDSG (Datenschutzklauseln und spezifische Garantien): Der Anforderungskatalog ist entweder zu streichen oder dann entsprechend anzupassen, indem „mindestens“ durch „je nach den Umständen“ zu ersetzen ist.

Art. 13 E-VDSG (Modalitäten der Informationspflichten): Auch hier fehlt es an der entsprechenden gesetzlichen Grundlage, indem das nDSG keine Informationspflicht des „Auftragsbearbeiter“ vorsieht. Die Regelung betreffend Piktogramme macht nicht wirklich Sinn und kann sogar zu Rechtsunsicherheit führen, weshalb der Artikel zu streichen ist.

Art. 15 E-VDSG (Information bei der Bekanntgabe von Personendaten): Für die darin vorgesehene Informationspflicht für die Verantwortlichen und Auftragsbearbeiter fehlt es an der gesetzlichen Grundlage, und die Bestimmung ist in dieser Form kaum praktikabel, weshalb sie entweder für private Datenbearbeiter anzupassen oder ganz zu streichen ist.

Art. 16 E-VDSG (Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten): Auch hier fehlt es an der entsprechenden gesetzlichen Grundlage im nDSG, weshalb der Artikel gestrichen werden sollte.

Art. 17 E-VDSG (Überprüfung einer automatisierten Einzelentscheidung): Diese Norm beruht auf dem ausführlichen Art. 21 nDSG. Sie will verhindern, dass betroffene Personen, die ihre gesetzlichen Rechte wahrnehmen, nicht benachteiligt werden. Es fragt sich jedoch, was mögliche Benachteiligungen sein könnten? Hier wäre die Auflistung von konkreten Beispielen hilfreich.

Art. 18 E-VDSG (Form und Aufbewahrung der Datenschutz-Folgeabschätzung): Die Datenschutz-Folgeabschätzung ist ein äusserst sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen des nDSG dar. Falls sich aus einer missbräuchlichen Datenbearbeitung Schäden für die betroffene Person ergeben und sich in der Folge Haftungsfragen stellen, kann die Datenschutz-Folgeabschätzung als Dokument dazu dienen, entsprechende Haftungsansprüche zu prüfen. Dementsprechend sollte die Aufbewahrungsfrist auf fünf Jahre verlängert werden. Zudem sollte „Schriftlichkeit" angepasst werden mit „in geeigneter Weise" oder „in Textform".

Art. 19 Abs. 5 E-VDSG (Meldung von Verletzungen der Datensicherheit): Die Dokumentation des EDÖB kann im Falle von Haftungsansprüchen relevant sein; eine Aufbewahrungsfrist von drei Jahren ist zu kurz und sollte auf fünf Jahre verlängert werden (s. auch Bemerkung zu Art. 18 E-VDSG).

Art. 20 E-VDSG (Modalitäten): Die Modalitäten zum Auskunftsbegehren sollten so geregelt werden, dass es problemlos für die betroffene Person ist, ihr Auskunftsrecht in angemessenen Abständen wahrzunehmen. Weiter wichtig ist, dass dieses Instrument nicht zum Rechtsmissbrauch benutzt wird.

Die Auskunft kann wiederum als Dokument bei Haftungsfragen dienen und die Auskunftspflicht sollte deshalb auf fünf Jahre verlängert werden (s. auch Bemerkung zu Art. 18 E-VDSG). Zudem sollte die Auskunft „im Grundsatz nachvollziehbar sein", und zwar nicht nur für die betroffene Person.

Art. 21 E-VDSG (Zuständigkeit): Es stellt sich die Frage, wie die Auskunft erfolgt, wenn mehrere Verantwortliche gemeinsam die Daten bearbeitet haben. Abgrenzungsschwierigkeiten sind ein bekanntes Problem zwischen gemeinsamen Verantwortlichen; dementsprechend wäre es sinnvoll, ein Regelwerk zu erarbeiten, welches verhindert, dass der betroffenen Person aus dieser Konstellation Nachteile erwachsen, wie beispielsweise ein Herumgeschiebe der Verantwortlichkeiten oder eine lückenhafte Auskunft. Es sollte deshalb präzisiert werden: „Sind für die Bearbeitung von Personendaten mehrere *gemeinsam* verantwortlich....".

Art. 25 E-VDSG (Datenschutzberaterin oder Datenschutzberater): Der Aufgabenbereich für Datenschutzberater, resp. Datenschutzberaterinnen ist rudimentär normiert. Hier sollte neben der Erwähnung der Mitwirkung an der Datenschutz-Folgenabschätzung die datenschutzfördernden Aufgaben der Datenschutzbeauftragten Person bei privaten Organisationen und Unternehmen thematisiert werden, beispielsweise im Sinne einer Obliegenheit. Wie bereits unter Art. 7 E-VDSG erwähnt, sollten Datenschutzberatende vermehrt präventiv tätig sein, sei es bei der Implementierung eines Datenschutz-Management-Systems, bei der Anschaffung neuer IT-Systeme oder bei der Schulung des Personals. Es empfiehlt sich deshalb, die Aufgaben der Datenschutzberaterin oder des Datenschutzberaters genauer zu präzisieren.

Art. 31 E-VDSG: Der Begriff „sogleich" ist zu ungenau und sollte durch „rechtzeitig" ersetzt werden.

Art. 32 E-VDSG: Abgesehen davon, dass Meldungspflichten in der Regel vor allem einen bürokratischen Mehraufwand ohne entsprechenden Nutzen für die Betroffenen bedeuten, sollte diese Bestimmung aufgrund der fehlenden gesetzlichen Grundlage gestrichen werden.

Art. 39 E-VDSG (Mitteilung von Richtlinien und Entscheiden): Es stellt sich die Frage, weshalb die Bundesverwaltung ihre Richtlinien dem EDÖB in anonymisierter Form mitzuteilen hat (vgl. Absatz 1).

Richtlinien zum Datenschutzgesetz sind Rahmenbedingungen, die an mehrere Adressaten gerichtet werden und diese sollten in der Regel dem Öffentlichkeitsprinzip unterstellt sein. Aus dem bisherigen Art. 32 Abs. 2 zweiter Satz VDSG lässt sich u.E. nach Wortlaut und Satzstellung nur ableiten, dass Entscheide in anonymisierter Form dem EDÖB mitzuteilen sind.

Wie bereits eingehend erwähnt, sollte eine Verordnung die im entsprechenden Gesetz geregelten Grundsätze praxisbezogen präzisieren und nicht losgelöst davon neue Grundsätze definieren, was leider in der E-VDSG nicht konsequent erfolgt ist. Auch wäre es für die mit der Umsetzung in der Praxis Betroffenen sinnvoll und hilfreich, wenn die Bestimmungen nicht allzu weit von der auch in der Schweiz oft geltenden DSGVO abweichen würden.

Im Namen des Datenschutz-Vorstands

Cordula E. Niklaus, Co-Präsidentin