DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Per Mail an: jonas.amstutz@bj.admin.ch

Ort, Datum	Bern, 14. Oktober 2021	Direktwahl	031 335 11 59
Ansprechpartnerin	Cheryl von Arx	E-Mail	cheryl.vonarx@hplus.ch

Revision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG): Vernehmlassung
Stellungnahme H+

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

An seiner Sitzung vom 23. Juni 2021 hat der Bundesrat das Vernehmlassungsverfahren zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) eröffnet. H+ bedankt sich für die Möglichkeit zur Stellungnahme. Gerne lassen wir Ihnen unsere Stellungnahme hiermit fristgerecht zugehen.

H+ Die Spitäler der Schweiz ist der nationale Verband der öffentlichen und privaten schweizerischen Spitäler, Kliniken und Pflegeinstitutionen. Uns sind 208 Spitäler, Kliniken und Pflegeinstitutionen als Aktivmitglieder an 343 Standorten sowie über 150 Verbände, Behörden, Institutionen, Firmen und Einzelpersonen als Partnerschaftsmitglieder angeschlossen. Wir vertreten über 200‘000 Arbeitsverhältnisse.

Inhaltsverzeichnis der Stellungnahme

1. Einleitung

In der Herbstsession 2020 hat das Parlament das neue Datenschutzgesetz (nDSG) verabschiedet. Die Referendumsfrist lief im Januar 2021 unbenutzt ab. Damit dieses in Kraft treten kann, müssen die entsprechenden Ausführungsbestimmungen in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) angepasst werden.
Der E-VDSG basiert auf zahlreichen Delegationsnormen im revDSG und konkretisiert Bestimmungen des revDSG. Der vorliegende Entwurf zur Revision der Verordnung zum Bundesgesetz über den Datenschutz (Datenschutzverordnung, VDSG) verfolgt auf Basis des totalrevidierten Datenschutzgesetzes (nDSG) folgende Ziele: die Verbesserung der Transparenz bei der Datenbeschaffung- und verarbeitung sowie die Stärkung der Selbstbestimmung der betroffenen Personen über ihre Daten. Gleichzeitig soll die Totalrevision der Schweiz erlauben, das revidierte Datenschutzübereinkommen SEV 108 des Europarats zu ratifizieren sowie die Schengen-relevante Richtlinie (EU) 2016/680 über den Datenschutz in Strafsachen umzusetzen. Die vorgesehenen Änderungen der vorliegenden Ausführungsbestimmungen betreffen etwa die Bestimmungen über die Mindestanforderungen an die Datensicherheit, die Modalitäten der Informationspflichten und des Auskunftsrechts oder die Meldung von Verletzungen der Datensicherheit.

Grundsätzlich begrüsst H+ die Neuerungen, die das Datenschutzrecht den veränderten technologischen und gesellschaftlichen Verhältnissen anpasst und andererseits die Kompatibilität zu den neuen Rechtsgrundlagen des europäischen Datenschutzrechts sicherstellt. H+ musste gleichzeitig feststellen, dass der E-VDSG zahlreiche Bestimmungen enthält, welchen eine gesetzliche Grundlage fehlt, oder dass sie gar dem Willen des Gesetzgebers widersprechen.

> *«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).*

Die Verwaltung überdehnt ihre rechtsetzerische Kompetenz, indem sie auf dem Verordnungsweg unter dem Titel der Datensicherheit massgeblich die ganze Datenschutz-Governance als solche über das DSG hinaus auszubauen versucht. Damit ist die E-VDSG oft unnötig restriktiv. Sie würde zu einem massiven Mehraufwand für die Spitäler führen und bspw. auch die, notabene gesetzlich verankerte Pflicht, zur Sicherung, Verbesserung und Weiterentwicklung der Qualität von medizinischen Behandlungen unnötig weiter erschweren[1]. H+ billigt ein solches Vorgehen nicht. Es zeugt von wenig Gespür gegenüber dem politischen Prozess, wenn Regelungen in einer unselbstständigen Verordnung Eingang finden, die wohl formellgesetzlich zu regeln wären.

Zudem wurden Artikel von der bisherigen VDSG übernommen oder sind direkt an die DSGVO angelehnt, ohne sie aber inhaltlich und terminologisch in den Gesamtentwurf einzupassen.

Der E-VDSG verpasst es insgesamt, die Mindestanforderungen in einer Form zu konkretisieren, welche die heutigen Begrifflichkeiten und Anforderungen der Datensicherheit aufnehmen. Der bürokratische Aufwand, welcher mit der Umsetzung der vorliegenden Verordnung verbunden ist, entspricht nicht dem Verhältnismässigkeitsprinzip. Für die Verantwortlichen ergibt sich ein unübersichtlicher Detaillierungsgrad, der in keiner Weise Rücksicht auf die Realität der Spitäler nimmt.

[1] Mehr Informationen: 20200630_Positionierung_Qualitaetsentwicklung_Gesetzlicher_Rahmen_V1.0_D.pdf (hplus.ch)

H+ setzt sich ein für geeignete rechtliche Rahmenbedingungen, um qualitativ hohe medizinische Behandlungen und ein effizientes Spitalwesen zu fördern. Dabei spielen datenschutzrechtliche Aspekte unbestritten eine wichtige Rolle. **Im vorliegenden Fall gehen die datenschutzrechtlichen Vorschriften aber über das hinaus, was gewollt und geboten ist und stellen damit eine unnötige administrative Hürde dar, die den Spitalalltag massiv beeinflussen. Einmal mehr werden fundamentale demokratie-politische Grundsätze untergraben. H+ lehnt die vorliegende Vernehmlassungsvorlage deshalb ab.** Dies gilt insb. für die folgenden Regelungen, die keine Detailvorschriften sind, sondern in ihrer Bedeutung viel eher den im nDSG enthaltenen Bestimmungen gleichkommen:

- Bearbeitungsreglement privater Personen (Art. 4 E-VDSG)
- Information bei der Bekanntgabe von Personendaten (Art. 15 und 16 E-VDSG)
- Dokumentationspflichten (bspw. Art. 19 Abs. 5 und Art. 20 Abs. 5 E-VDSG)

2. Datensicherheit

2.1. Allgemeiner Teil

Mit den Bestimmungen zur Datensicherheit erfüllt der Bundesrat den gesetzlichen Auftrag, die Mindestanforderungen an die Datensicherheit auf Verordnungsstufe zu präzisieren (Art. 8 Abs. 3 nDSG). An diese Mindestanforderungen knüpft zudem die Strafnorm in Artikel 61 Buchstabe c nDSG an. Der Grad an Sicherheit, der eingehalten werden muss, damit die Strafnorm nicht verletzt wird, bestimmt sich dabei nach den Grundsätzen und Kriterien des vorliegenden, ersten Abschnittes. Im E-VDSG wurde auf ein starres Regime von Mindestanforderungen verzichtet, da sich keine allgemeingültigen Mindestanforderungen für jegliche Branchen festlegen lassen. Der Ansatz des E-VDSG beruht – entsprechend dem Gesetz – auf einem risikobasierten Ansatz: Je höher die Gefährdung für die Persönlichkeitsrechte und die Grundrechte des Einzelnen, desto höher die Anforderungen.

H+ lehnt die Bestimmungen in diesem Abschnitt ab, sofern ihnen eine gesetzliche Grundlage fehlt bzw. sie dem Willen des Gesetzgebers widersprechen. Die Bestimmungen sind zu detailliert und tragen damit der Vielfalt der Bearbeitungsaktivitäten und Situationen keine Rechnung. Regelungen nach dem Giesskannenprinzip bringen keine Rechtssicherheit, sondern bewirken eher das Gegenteil. Für H+ ist es unverständlich, dass verbreitet angenommen wird, dass mit engmaschiger Kontrolle und damit massiv mehr administrativem Aufwand automatisch eine bessere Durchsetzung des Datenschutzes erfolgt. Ganz im Sinne von «vor lauter Bäumen den Wald nicht mehr sehen» ist H+ der Auffassung, dass die vorliegenden Regelungen, am Ziel und Zweck für mehr Datensicherheit vorbeischiessen und die aktuell noch nicht abschätzbaren, negativen Folgen überwiegen.

2.2. Besonderer Teil

Art. 3 Abs. 1: Protokollierung

Kommentar: 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. Gemäss dem erläuternden Bericht besteht der Zweck der Protokollierung darin, dass Bearbeitungen von Personendaten nachträglich überprüfbar sind, so dass im Nachhinein festgestellt werden kann, ob Daten abhandengekommen sind oder gelöscht, vernichtet, verändert oder offengelegt wurden. Ausserdem geht es auch um die Gewährleistung der Zweckkonformität. So können sich aus der Protokollierung auch Hinweise ergeben, ob Personendaten zweckkonform bearbeitet wurden. Weiter können die Protokollierungen auch dazu dienen, Verletzungen der Datensicherheit aufzudecken und aufzuklären. Die Protokollierung hat hingegen nicht zum Ziel, die Nutzerinnen und Nutzer, die Personendaten bearbeiten, zu überwachen.
Diese Bestimmung ist aus Sicht der Spitäler in mehrfacher Hinsicht bedenklich:

- Sollte diese Bestimmung so umgesetzt werden, bedarf es eines riesigen Überwachungsapparats, welcher viele Ressourcen (finanziell wie auch personell) binden würde.
- Die Norm dient nicht primär der Protokollierung zur Gewährleistung der Datensicherheit, sondern vielmehr der nachträglichen Feststellung, ob es zu einer unbefugten Datenbearbeitung gekommen ist. Die Norm widerspricht damit dem Gesetz, weil sie sich zur Feststellung einer Verletzung der Datensicherheit[2] nicht eignet und damit unverhältnismässig ist.

[2] 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.

- Das Ergebnis einer Datenschutz-Folgenabschätzung (DSFA) wird in der Regel nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenbearbeitung. Das hat mit der Datensicherheit nichts zu tun. Folglich ist das Ergebnis der DSFA kein geeigneter Indikator, um das Risiko einer Verletzung der Datensicherheit festzustellen.

Punktuelle Pflichten zur Protokollierung mögen durchaus sinnvoll sein (bspw. zur Auswertung von Logs zu Analysezwecken); eine solche pauschale Norm lehnt H+ indessen klar ab, da sie schlicht unverhältnismässig ist. Die Erläuterungen des E-VDSG (so auch Art. 3 Abs. 3) bestätigen sogar, dass es (auch) um die Gewährleistung der zweckkonformen Bearbeitung geht. Das widerspricht klar dem Gesetzgebungsauftrag.

Art. 4: Bearbeitungsreglement von privaten Personen

Kommentar: Art. 4 E-VDSG enthält die Pflicht zur Erstellung eines Bearbeitungsreglements. Entsprechend dem risikobasierten Ansatz der Vorgabe der Datensicherheit soll ein Bearbeitungsreglement immer dann erstellt werden, wenn ein erhöhtes Risiko vorliegt. So müssen private Verantwortliche ein Bearbeitungsreglement für automatisierte Bearbeitungen erstellen, u.a. wenn sie umfangreich besonders schützenswerte Personendaten bearbeiten (Bst. a).
Systematisch wird dies bei der Datensicherheit geregelt, aber ein Bearbeitungsreglement ist offenkundig keine Datensicherheitsmassnahme, sondern dient der Einhaltung der Datenbearbeitungsgrundsätze und damit dem Datenschutz. Auch bei der vorliegenden Bestimmung fehlt dementsprechend die gesetzliche Grundlage (s. oben). Dabei steht der beträchtliche Aufwand für die Bewirtschaftung eines solchen Bearbeitungsreglements in keinem Verhältnis (massive Ausdehnung der Dokumentationspflichten, die weit über das Gebotene herausgehen).
Überdies gilt es folgende Punkte zu kritisieren:

- Die wesentlichen Angaben werden ohnehin bereits im Rahmen der in solchen Fällen erforderlichen Datenschutz-Folgenabschätzung dokumentiert, der Rest im ohnehin zu erstellenden Inventar.
- Auch die DSGVO sieht eine solche Regelung nicht vor (sog. «Swiss Finish»).
- Zweifellos können besonders heikle Datenbearbeitungen eine betriebsinterne Regelung erfordern. Dieser Aspekt ist jedoch über Art. 7 Abs. 1 revDSG bereits hinreichend geregelt.

Die Bestimmung ist damit unnötig restriktiv und aus Sicht von H+ zu streichen.

3. Pflichten des Verantwortlichen und des Auftragsbearbeiters

3.1. Allgemeiner Teil

Im 2. Kapitel werden die Informations- und Meldepflichten konkretisiert. Art. 13 Abs. 1 E-VDSG impliziert eine Informationspflicht des Auftragsbearbeiters, was auch aus dem erläuternden Bericht (S. 30) explizit hervorgeht. Das revDSG sieht aber keine Informationspflicht des Auftragsbearbeiters vor; gemäss Art. 19 revDSG besteht diese – richtigerweise – nur für den Verantwortlichen. Da das Gesetz keine solche Pflicht für den Auftragsbearbeiter vorsieht, kann sie auch nicht über die Verordnung eingeführt werden. Das gilt für alle Artikel im zweiten Kapitel gleichermassen, sofern sie Informationspflichten betreffen.

3.2. Besonderer Teil

Art. 15 und 16: Information bei der Bekanntgabe sowie über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten

Kommentar: Nebst der «Aktualität» und der «Zuverlässigkeit» der Personendaten wird im Rahmen der Informationspflicht bei der Bekanntgabe von Personendaten in *Artikel 15* neu die «Vollständigkeit» erwähnt. Mit anderen Worten dürfen die Daten, welche herausgegeben werden, nicht lückenhaft sein. Bei dieser Vorschrift beisst sich die Katze in den Schwanz: Der Empfänger ist selbst verpflichtet, die Bearbeitungsgrundsätze einzuhalten und angemessene Massnahmen zu treffen, sich über die Richtigkeit der Daten zu vergewissern. Eine entsprechende Information durch die übermittelnde Person unterläuft dies bzw. macht eine der möglichen Vergewisserungsmassnahmen zum allein gültigen Massstab. Dies widerspricht dem Gesetz. Die Regelung ist überdies in der Praxis nicht umsetzbar; sind Daten lückenhaft, dürfte der Auftragsbearbeiter sie also gar nicht herausgeben bzw. er soll etwas bekanntgeben, das er gar nicht hat.

Die Pflicht des Datenverantwortlichen, die Empfänger über sämtliche Veränderungen in den Personendaten (Berichtigung, Löschung oder Vernichtung der Bearbeitung) zu informieren, wie sie in *Artikel 16* E-VDSG vorgesehen ist, widerspricht dem Willen des Gesetzgebers: Die Bestimmung war bereits im Entwurf des revDSG vorgesehen und wurde vom Parlament gestrichen. Sie kann daher nicht über die revidierte Verordnung eingeführt werden.
Sollte die Bestimmung wie vorgesehen umzusetzen sein, würde dies, gerade für die Spitäler, einen enormen, gar unüberblickbaren, Aufwand bedeuten.

Die beiden Normen sind aus Sicht von H+ zu streichen, weil sie einen enormen Aufwand bedeuten würden und praktisch nicht umsetzbar sind.

Art. 19 Abs. 5

Kommentar: Bereits die Botschaft zum revDSG hielt fest, dass keine allgemeine Dokumentationspflicht eingeführt werden soll (S. 6978). Diese soll nun aber mittels dem vorliegenden Verordnungsentwurf durch die Hintertür verankert werden. Das würde aber die allgemeingültigen gesetzgeberischen Regeln unterlaufen.
Des Weiteren bleibt freilich unklar, was der Nutzen der Dokumentations- und Auskunftspflicht sein soll, wenn sich aus der Systematik klar ergibt, dass nur meldepflichtige Verletzungen zu dokumentieren sind. Wird eine Verletzung gemeldet und ist diese für den EDÖB von Interesse, wird er den Sachverhalt untersuchen, aber kaum später darauf zurückkommen. Der Nutzen wäre also auch für den EDÖB keinen.

Dasselbe gilt im Übrigen auch für Art. 20 Abs. 5 bei der Pflicht zur Dokumentation der Verweigerungs-, Einschränkungs- und Aufschubsgründen im Falle eines Auskunftsbegehrens. *Diese Norm ist im Übrigen auch wenig zweckmässig. 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 (längere Aufbewahrungszeit bzw. höhere Kadenz der Datenbeantwortung als notwendig).*

Die beiden Bestimmungen bringen keinen Mehrwert, sind operativ ausgesprochen aufwendig und haben keine gesetzlichen Grundlagen. Sie sind deshalb zu streichen.

4. Weiteres

Im Übrigen schliessen wir uns der allgemeinen Stellungnahme des Vereins für Unternehmens-Datenschutz (VUD) an.

* * * * *

Wir danken Ihnen für die Aufnahme unserer Anliegen und stehen Ihnen für ergänzende Auskünfte gerne zur Verfügung.

Freundliche Grüsse

Anne Bütikofer
Direktorin