www.jusletter.ch

Christian Peter

DSGVO und E-DSG fordern Schweizer Spitäler, Praxen, Heime und Spitex

Eine medizinische Behandlung ohne Vertrauen ist nicht möglich und Vertrauen bedingt einen respektvollen Umgang mit den Patientendaten. Daher ist der Datenschutz bei Schweizer Spitälern, Praxen, Heimen und der Spitex ein Dauerthema. 2018 wird jedoch speziell: Am 25. Mai 2018 muss die Europäische Datenschutz-Grundverordnung umgesetzt sein und im Herbst 2018 könnte das revidierte nationale Datenschutzgesetz in Kraft treten. Grund genug aufzuzeigen, was dies in der Praxis bedeutet.

Beitragsarten: Beiträge
Rechtsgebiete: Datenschutz; Europarecht; Gesundheitsrecht

Zitiervorschlag: Christian Peter, DSGVO und E-DSG fordern Schweizer Spitäler, Praxen, Heime und Spitex, in: Jusletter 26. Februar 2018

ISSN 1424-7410, https://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Die europäische Datenschutz-Grundverordnung

[Rz 1] Im Mai 2016 trat die europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft. Bis im Mai 2018 muss sie umgesetzt werden. Weil die Revision des eidgenössischen Datenschutzgesetzes (DSG), das diese Verordnung teilweise umsetzen soll, bis Mai 2018 nicht in Kraft treten wird, wird von Datenschutzdienstleistern darauf hingewiesen, dass bereits die EU-DSGVO für Schweizer Betriebe Neuerungen bringen könnte. Da die EU-Verordnung drakonische Bussen für Verstösse vorsieht, werden viele Betriebe aufgeschreckt.

[Rz 2] Zentral ist die Frage, ob die EU-DSGVO überhaupt auf Schweizer Spitäler oder anderen Leistungserbringer anwendbar ist. Die europäische Regelung hat zum Ziel, den Schutz von EU-Bürgern auch durch Dienstleistungserbringer ausserhalb der EU sicherzustellen. Die Bürger sollen den Schutz nicht verlieren, nur weil ein Dienstleister nicht in der EU angesiedelt ist (im Fokus stehen Datenbearbeiter wie Facebook, Google, Apple etc.), die Dienstleistungen jedoch trotzdem in der EU angepriesen wird (Marktortprinzip).

1.1. Allgemein

[Rz 3] Die EU-DSGVO findet auf die Verarbeitung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter Anwendung, die personenbezogene Daten betroffener Personen, die sich in der EU befinden, verarbeiten und die Datenverarbeitung im Zusammenhang damit steht, diesen Personen in der Union Waren oder Dienstleistungen anzubieten oder das Verhalten von Privatpersonen in der Union zu verfolgen. Solche Unternehmen mit Sitz ausserhalb der EU haben dieselben Regeln anzuwenden wie Unternehmen mit Sitz in der EU. Damit wird der umfassende Schutz der Rechte von Bürgern in der Union sichergestellt und es werden auf diese Weise gleiche Wettbewerbsbedingungen für EU-Unternehmen und Nicht-EU-Unternehmen geschaffen.[1] Die-

[1] Thomas Zerdick, in: Eugen Ehmann und Martin Selmayr (Hrsg.), DS-GVO, Datenschutzgrundverordnung, Kommentar, Art. 3 Rz. 2.

ses «Markortprinzip»[2] ist auch aus dem europäischen Wettbewerbs- und Verbraucherschutzrecht bekannt.[3] Der Grundrechtsschutz soll auch im Internetzeitalter Bestand haben.[4]

1.2. Das Marktortprinzip

[Rz 4] Kennzeichen des Marktortprinzips ist, dass danach das Recht desjenigen Orts anwendbar ist, an dem final in das Markgeschehen eingegriffen und auf die Marktgegenseite eingewirkt wird.[5]

[Rz 5] Dies ist dann der Fall, wenn der Verantwortliche oder Auftragsverarbeiter es «offensichtlich beabsichtigt», betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten. Damit kommt es massgeblich auf die Ausrichtung des Angebots an. Dieses Kriterium ist erfüllt, wenn die betroffenen Personen vom Verantwortlichen oder Auftragsverarbeiter spezifisch im Sinne eines «Targeting» adressiert wird.[6]

[Rz 6] Die Vorschrift zielt primär auf die Verarbeitung personenbezogener Daten im Rahmen des Internets ab.[7] Ein sogenanntes «Forum Shopping» soll verhindert werden. Das heisst, dass ein Anbieter sich nicht durch die Wahl eines Sitzes ausserhalb der EU allzu leicht der Beachtung der datenschutzrechtlichen Vorgaben in der EU entziehen können soll.[8]

1.3. Art. 3 EU-DSGVO

[Rz 7] So erstreckt sich die Anwendbarkeit der EU-DSGVO gemäss Art. 3 Abs. 2 auf Verarbeitungen personenbezogener Daten von Personen, die sich in der Union befinden, und auf Angebote von Waren oder Dienstleistungen in der Union sowie auf beobachtetes Verhalten in der Union.[9]

1.3.1. Personen in der EU

[Rz 8] Ob «sich in der Union befinden» bedeutet, dass der Aufenthalt in der Union ein dauerhafter oder auch ein vorübergehender sein kann, ist umstritten. Naheliegender erscheint es jedoch, dass ein vorübergehender Aufenthalt ausreicht.[10] Klar ist jedoch, und dies ist für unsere Frage von zentralem Interesse, dass sich die betroffene Person im Zeitpunkt der fraglichen Datenverarbeitung in der Union aufhalten muss.[11]

---

2 Vergleichbare Prinzipien gibt es auch im amerikanischen oder japanischen Datenschutzrecht.

3 Manuel Klar, in: Jürgen Kühling und Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung, Kommentar, C.H. Beck, 2017, Art. 3, Rz. 6; Franziska Sprecher, Quantied Self: Rechtsentwicklungen – Europa gibt den Takt vor, in: Jusletter 11. Dezember 2017, Rz. 18.

4 Zerdick (Fn. 1), Art. 3 Rz. 1.

5 Klar (Fn. 3), Art. 3 Rz. 7.

6 Klar (Fn. 3), Art. 3 Rz. 9.

7 Klar (Fn. 3), Art. 3 Rz. 10.

8 Klar (Fn. 3), Art. 3 Rz. 18.

9 Klar (Fn. 3), Art. 3 Rz. 22.

10 Der Verordnungsgeber ist bewusst vom ursprünglichen «ansässig» abgewichen, das im Entwurf der Kommission, des Parlaments und des Rates stand. Zerdick (Fn. 1), Art. 3 Rz. 16.

11 Klar (Fn. 3), Art. 3 Rz. 63; Zerdick (Fn. 1), Art. 3 Rz. 16.

1.3.2. Angebot von Waren und Dienstleistungen in der EU

[Rz 9] Nach Art. 3 Abs. 2 Bst. a EU-DSGVO muss die Verarbeitung personenbezogener Daten im Zusammenhang mit einem Angebot von Waren oder Dienstleistungen an Personen in der Union stehen. Das Angebot muss nicht aktiv ausgesprochen werden, sondern kann auch ein blosses passives Bereithalten eines Angebots auf einer Internetseite sein.[12] Der Ort, an dem die Dienstleistung erbracht wird, ist unerheblich.

[Rz 10] Die EU-DSGVO definiert nicht, was unter einer Ware oder einer Dienstleistung zu verstehen ist. Daher muss von einem umfassenden Waren- und Dienstleistungsbegriff ausgegangen werden.[13] Als Beispiele für eine Dienstleistung im Sinne von Art. 3 Abs. 2 Bst. a EU-DSGVO lassen sich im Internet buchbare Reisen, Videostreamingdienste, Cloud-Angebote, Online-Pressediente oder Vergleichsportale nennen.

[Rz 11] Der rein zu Präsentationszwecken erfolgte Webauftritt eines Unternehmens stellt keine Dienstleistung in diesem Sinne dar. Auch ist es nicht ausreichend, mittels einer Webseite die Dienste lediglich zugänglich zu machen.[14]

[Rz 12] Die Waren oder Dienstleistungen müssen zudem zwingend «in der Union» angeboten werden. Das heisst, dass das Angebot im Sinne des Marktortprinzips auf Personen in der Union ausgerichtet sein muss.[15]

[Rz 13] Es ist gemäss dem Erwägungsgrund 23[16] entscheidend, ob es der Verantwortliche «offensichtlich beabsichtigt» den Personen in der Union Dienstleistungen anzubieten.[17] Diese Voraussetzungen sind nicht erfüllt, wenn man bloss faktisch die Möglichkeit hat, auf einer Webseite eine Bestellung abzugeben.

[Rz 14] Selbst in Bezug auf Spitäler, welche ihren Webauftritt auf eine internationale Klientschaft ausrichten, bedeutet dies nicht, dass ein Webauftritt alleine, über den ein Behandlungsvertrag geschlossen werden könnte, die EU-DSGVO zur Anwendung bringt. Eine deutlich erkennbare Ausrichtung des Angebotes auf das Markgebiet der Union, resp. mindestens eines Mitgliedstaates, ist erforderlich. Mehrdeutigkeiten, wie z.B. ein Webauftritt in der Schweiz auf Französisch, zielt nicht offensichtlich auf französische Kundschaft, sondern evtl. auch auf Kunden aus der Romandie.[18]

[Rz 15] Die Verwendung von mitgliedstaatspezifischen Top-Level Domains (z.B. «.de», «.fr», «.it» oder «.at») können jedoch zum Ausdruck bringen, dass eine Dienstleistung in der EU angeboten wird. Ebenso Anfahrtsbeschreibungen von einem oder mehreren Mitgliedstaaten aus zum Ort der Niederlassung oder die Wiedergabe von Kundenbewertungen aus der EU.[19]

[Rz 16] Wird eine Sprache verwendet, welche auch in Ländern ausserhalb der Union üblich ist, wie z.B. englisch, französisch oder spanisch, kann man ohne andere Anhaltspunkte nicht per se

12 Klar (Fn. 3), Art. 3 Rz. 67.

13 Zerdick (Fn. 1), Art. 3 Rz. 17.

14 Carlo Pilz, in:Peter Gola (Hrsg.), Datenschutz-Grundverordnung, C.H. Beck 2017, Art. 3 Rz. 28.

15 Klar (Fn. 3), Art. 3 Rz. 80.

16 Die Erwägungsgründe sind Erläuterungen zum Rechtstext, mit dem aufgezeigt werden soll, welche Überlegungen zum Erlass des Rechtsaktes geführt haben.

17 Zerdick (Fn. 1), Art. 3 Rz. 18.

18 Vgl. auch das Beispiel bei Pilz (Fn. 14), Art. 3 Rz. 28.

19 Klar (Fn. 3), Art. 3 Rz. 84.

von einer Anwendbarkeit der EU-DSGVO ausgehen, weil es an der geforderten «Offensichtlichkeit» mangelt.

[Rz 17] Eine Disclaimer, dass sich das Angebot nicht an Personen richtet, die sich in der EU aufhalten, führt mit Sicherheit zur Nichtanwendbarkeit der EU-DSGVO.[20]

1.3.3. Auswirkungen auf Schweizer Spitäler und andere Leistungserbringer

[Rz 18] Lässt sich ein europäischer Tourist in einem Schweizer Spital behandeln oder begibt sich ein europäischer Konsument in die Schweiz (ohne dass das Spital seine Dienstleistungen im europäischen Markt aktiv anbot), um die Leistung in Anspruch zu nehmen, kommt die EU-DSGVO nicht zur Anwendung. In der Terminologie der Union handelt es sich um die sog. passive Dienstleistungsfreiheit[21]. Da der Kunde sich aus eigener Entscheidung in den Drittstaat begibt, muss er die dortigen Rechtsregeln und das Schutzniveau hinnehmen.[22] Auch wird es so sein, dass die mit der Behandlung verbundene Datenbearbeitung zu einem Zeitpunkt stattfindet, zu der der Betroffene sich eben gerade nicht in der EU befindet (sondern in der Schweiz).

[Rz 19] Auch nicht zur Anwendung gelangt die EU-Verordnung, wenn sich ein Spital nicht auf den europäischen Markt ausrichtet. Vielen Häusern geht der internationale Charakter ihre Tätigkeit ab, welcher ein Anhaltspunkt für die Ausrichtung auf den europäischen Markt sein könnte.

[Rz 20] Dass das Personal der Spitäler oder anderer Leistungserbringer aus europäischen Ländern stammt, führt nicht zu einer Anwendbarkeit der EU-DSGVO.

[Rz 21] Spitäler hingegen, welche sich mit ihrem Angebot explizit an europäische Patienten richten, in dem sie zum Beispiel die europäischen Kunden direkt mit einem Internetauftritt z.B. in schwedischer[23] Sprache ansprechen und mittels einem «international Office» europäische Kunden speziell betreuen, sowie Häuser, welche für ihre Forschungsvorhaben Probanden aus der EU rekrutieren, müssen davon ausgehen, dass dieses Vorhaben zu einer Anwendung der EU-DSGVO führt.

[Rz 22] Die extraterritoriale Wirkung der EU-DSGVO lässt sich völkerrechtlich nur legitimieren, wenn ein hinreichender Bezug resp. ein ausreichender Anknüpfungspunkt zum eigenen Hoheitsgebiet, zum eigenen Recht oder zu den eigenen Angehörigen besteht.[24] Eine solche ausreichende Anknüpfung liegt in denjenigen Fällen eben nicht vor, wo der Kunde resp. der Patient aus eigenem Antrieb den europäischen Rechtsraum verlässt und von einem Angebot profitiert, das sich nicht an den europäischen Markt richtet.

[Rz 23] Wichtig ist noch festzuhalten, dass die räumliche Anwendbarkeit nicht durch Rechtswahlklauseln abdingbar ist.[25]

---

20 Klar (Fn. 3), Art. 3 Rz. 82.

21 Unter der passiven Dienstleistungsfreiheit versteht man das Recht, sich zur Entgegennahme einer Dienstleistung in einen anderen Staat zu begeben.

22 So Rolf Sethe für Finanzdienstleistungen; siehe Rolf Sethe, Das Drittstaatenregime von MiFIR und MiFID II, in: SZW / RSDA 6/ 2014, S. 617 f.

23 Bei einem Auftritt in englischer Sprache müssten noch zusätzliche Elemente hinzukommen, damit klar ersichtlich wird, dass z.B. nicht ausschliesslich amerikanische Patienten akquiriert werden sollen.

24 Astrid Epiney / Markus Kern, in: Astrid Epiney / Daniela Nüesch (Hrsg.), Die Revision des Datenschutzes in Europa und die Schweiz, Schulthess 2016, S. 49.

25 Klar (Fn. 3), Art. 3, Rz. 105.

[Rz 24] Somit droht die Anwendbarkeit der EU-DSGVO weniger aufgrund des Marktortprinzips als vielmehr aufgrund dessen, dass Schweizer Spitäler, Heime, Praxen oder die Spitex die Besucher ihrer Internetseiten beobachten.

1.4. Beobachtung von EU-Kunden

1.4.1. Beobachten von Besuchern der eigenen Internetseiten

[Rz 25] Nach Art. 3 Abs. 2 lit. b erstreckt sich der Anwendungsbereich der EU-DSGVO auch auf die Datenverarbeitung durch ausserhalb der EU niedergelassene Verantwortliche, die im Zusammenhang steht mit der Beobachtung des Verhaltens von Personen, die sich in der Union befinden und deren Verhalten in der Union erfolgt.[26]

[Rz 26] Was konkret mit dem «Beobachten» gemeint ist, versucht der Gesetzgeber in Erwägungsgrund 24 näher zu erläutern:

[Rz 27] «Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.»

[Rz 28] Es wird deutlich, dass der Gesetzgeber das Online-Umfeld im Blick hatte.[27] Als «Beobachten» gilt jedoch nur ein aktives Verhalten der Verantwortlichen. Es müssen bewusst Vorkehrungen getroffen werden, um das Verhalten der Betroffenen zu beobachten. Es ist nötig, dass die Beobachtung eine gewisse Intensität aufweist. Massnahmen, die nur punktuell ergriffen werden, stellen keine Beobachtung dar, da nur auf eine bestimmte Dauer ausgelegte Beobachtung ein erfolgreiches «Tracking» oder «Profiling» möglich macht.[28]

[Rz 29] Insbesondere fallen jegliche Formen des Trackings (Beobachten, Sammeln, Auswerten des Surfverhaltens betroffener Personen im Internet) und des Profilings (Erstellung von Profilen von Kunden, Mitarbeitern oder anderen, um bestimmte persönliche Aspekte wie Leistung, Gesundheit, Aufenthaltsort etc. zu bewerten oder Vorhersagungen zu treffen) im Internet durch Analyse-Tools, die wie etwa Cookies die individuelle Rückverfolgbarkeit der Nutzer ermöglichen oder zum Zweck der individuellen Werbung (targeted Advertising) erfolgen, unter die Vorschrift.[29] Zudem sind Social Plugins und sonstige Schaltflächen im Internet erfasst, die wie der «Like-Button» von Facebook die von betroffenen Personen aufgesuchten Internetseiten registrierten.[30]

---

26 Klar (Fn. 3), Art. 3, Rz. 90.

27 Pilz (Fn. 14), Art. 3 RZ. 31; Klar (Fn. 3), Art. 3 Rz. 92. Eine Verhaltensbeobachtung innerhalb eines unternehmensinternen Netzwerks fällt nicht unter die DS-GVO.

28 Klar (Fn. 3), Art. 3 Rz. 94.

29 Kurzpapier 7 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Marktortprinzip: Regelungen für außereuropäische Unternehmen, Stand: 26. Juli 2017.

30 Klar (Fn. 3), Art. 3 Rz. 98; Zerdick (Fn. 1), Art. 3 Rz. 19.

1.4.2. Auswirkungen auf Schweizer Spitäler, Heime, Praxen und Spitex

[Rz 30] Die meisten Spitäler, Praxen, Heime und die Spitex setzen sog. Cookies ein, um das Verhalten der Besucher ihrer Internetseiten beobachten und analysieren zu können. Da noch keine Praxis besteht, wie die europäischen Behörden die Anwendbarkeit der EU-DSGVO interpretieren, erscheint es ratsamen, dass Schweizer Spitäler, Praxen, Heime und die Spitex darauf verzichten, die Besucher ihrer Internetseite zu tracken oder Profiling zu betreiben. Sei dies, dass sie komplett darauf verzichten oder aber mit Hilfe von Geo-Lokalisierungstools europäische Besucher im Sinne eines «dis-targetings» vom Tracking und Profiling ausnehmen.[31]

2. Die Totalrevision des schweizerischen Datenschutzgesetzes

2.1. Anwendbarkeit des nationalen Rechts

[Rz 31] Welches Recht auf Spitäler, Heime, Praxen oder die Spitex zur Anwendung gelangt, ist insbesondere für private Listenspitäler umstritten. Bernhard Rütsche hat in seinem Gutachten schlüssig aufgezeigt, dass nicht nur öffentliche Listenspitäler dem kantonalen Datenschutzrecht unterstehen, sondern auch private. Nicht stationär tätige Leistungserbringer hingegen und Spitäler ohne Leistungsauftrag unterliegen dem nationalen Recht.[32]

2.2. Einleitung

[Rz 32] Die nachfolgenden Aussagen zu den Normen des E-DSG basieren zum Grossteil auf der Botschaft des Bundesrates zum Entwurf.[33]

[Rz 33] Mit dem Gesetzesentwurf sollen hauptsächlich zwei Zielsetzungen verwirklicht werden: Einerseits sollen die Schwächen des Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung und des Alters[34] der Norm entstanden sind. Andererseits soll die Revision den Entwicklungen auf der Ebene des Europarats[35] und der Europäischen Union[36] Rechnung tragen.

- Neu soll auf den Schutz der Daten juristischer Personen verzichtet und der Geltungsbereich des Gesetzes entsprechend angepasst werden.
- Generell wird die Transparenz der Bearbeitung verbessert.
- Die Revision soll die Selbstregulierung bei den Verantwortlichen fördern.

---

31 Klar (Fn. 3), Art. 3 Rz. 101.

32 Eingehend zu dieser Frage: Bernhard Rütsche, Datenschutzrechtliche Aufsicht über Spitäler / Surveillance de la protection des données dans les hôpitaux, Digma Schriften zum Datenrecht, 6, Schulthess, Zürich 2012.

33 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941.

34 Beim Inkrafttreten des DSG 1992 gab es z.B. Google noch nicht.

35 Protokoll zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten.

36 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts. Nur die Richtlinie ist Teil des Schengen-Acquis.

- Schliesslich werden auch die Strafbestimmungen des Gesetzes in verschiedener Hinsicht verschärft. Dies erfolgt insbesondere, weil der Datenschutzbeauftragte, anders als seine europäischen Amtskollegen, keine Verwaltungssanktionen auferlegen darf.

[Rz 34] Dies alles auch mit dem Ziel, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass das schweizerische Datenschutzniveau angemessen ist.

2.3. Die 7 Leitlinien der Revision

[Rz 35] Die Revision orientiert sich an sieben Leitlinien, auf denen die verschiedenen Neuerungen beruhen:

2.3.1. Erste Leitlinie: Risiko

[Rz 36] Eine erste Leitlinie der Revision bildet der risikobasierte Ansatz. Der Revisionsentwurf orientiert sich konsequent an den potenziellen Risiken für die betroffenen Personen.

[Rz 37] Dementsprechend sind beispielsweise die Pflichten von «Verantwortlichen» (dies ist eine neue Bezeichnung und ersetzt den bisherigen Begriff des «Inhabers der Datensammlung»), deren Aktivitäten mit einem erhöhten Risiko verbunden sind (z. B. Unternehmen, deren Haupttätigkeit in der Datenbearbeitung besteht), strenger als jene von Verantwortlichen, deren Aktivitäten ein geringeres Risiko darstellen (z. B. Datenbearbeitungen, die auf eine Kundendatei ohne besonders schützenswerte Daten beschränkt sind).

[Rz 38] Daraus resultiert, dass Spitäler aufgrund ihres grossen Risikos mit strengeren Pflichten konfrontiert sind; dies insbesondere bei der Pflicht zum «Privacy by design» und der Informationssicherheit.

2.3.2. Zweite Leitlinie: technologieneutraler Charakter der Revisionsvorlage

[Rz 39] Wie das derzeit geltende Gesetz soll auch das E-DSG so weit wie möglich alle Technologien gleichberechtigt behandeln.

2.3.3. Dritte Leitlinie: Modernisierung der Terminologie

[Rz 40] Mit der neuen Terminologie soll insbesondere die Vereinbarkeit mit dem Recht der Europäischen Union verbessert werden.

[Rz 41] Der Begriff «Verantwortlicher» ersetzt den Begriff «Inhaber der Datensammlung» und neu steht der Begriff «Profiling» für den helvetischen Begriff «Persönlichkeitsprofil». Zudem werden unter dem Begriff «besonders schützenswerte Personendaten» neu auch genetische und biometrische Daten subsumiert.

2.3.4. Vierte Leitlinie: Verbesserung des grenzüberschreitenden Datenverkehrs

[Rz 42] Die geltende Regelung für die grenzüberschreitende Bekanntgabe von Daten wird teilweise ausgebaut.

[Rz 43] Der Grundsatz, wonach Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn kein angemessener Schutz gewährleistet ist, wird aufgrund der damit verbundenen Rechtsunsicherheit ersetzt. Daten dürfen zukünftig ins Ausland übermittelt werden, wenn der Bundesrat per Verordnung festgestellt hat, dass das empfangende Land oder internationale Organ einen angemessenen Datenschutz gewährleistet. Liegt kein solcher Beschluss vor, sieht das E-DSG verschiedene Möglichkeiten vor, mit denen ein geeigneter Schutz gewährleistet werden kann, sodass die Bekanntgabe ins Ausland dennoch möglich ist. Im Spitalumfeld ist weiterhin zu beachten, dass das strafrechtliche Berufsgeheimnis für eine Weitergabe in jedem Fall die Einwilligung des Patienten voraussetzt.

2.3.5. Fünfte Leitlinie: Stärkung der Rechte der betroffenen Personen

[Rz 44] Diese Leitlinie ist besonders bedeutsam: die betroffenen Personen sollen besser über ihre Daten bestimmen können und ihnen soll es leichter fallen, den Nutzen ihrer Daten zu kontrollieren.

2.3.6. Sechste Leitlinie: Pflichten der Verantwortlichen präzisiert und stärker auf den Schutz der betroffenen Person ausgerichtet

[Rz 45] Die Informationspflicht ist im Entwurf gegenüber dem geltenden Recht umfassender ausgestaltet. Zudem werden die Verantwortlichen dazu verpflichtet, bei gewissen Arten von Bearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen. Ebenso sollen technische Vorkehren für eine datenschutzfreundliche Ausgestaltung von Systemen sorgen.

2.3.7. Siebte Leitlinie: Stärkung der Kontrolle durch den Datenschutzbeauftragten

[Rz 46] Die Stellung und Unabhängigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) soll gestärkt werden. Seine Befugnisse sollen künftig mit den Befugnissen der entsprechenden ausländischen Kontrollbehörden vergleichbar sein. Weiterhin wird er jedoch, im Gegensatz zu den meisten seiner Kolleginnen und Kollegen im europäischen Ausland, nicht befugt sein, Verwaltungssanktionen auszusprechen. Dies wird ausgeglichen, indem der strafrechtliche Teil ausgebaut wird.

2.4. Inhalt der Revision

2.4.1. Zweck

[Rz 47] Der Zweck ändert sich nicht. Das DSG konkretisiert weiterhin das in Art. 13 Abs. 2 der Bundesverfassung (BV) festgehaltene Recht auf informationelle Selbstbestimmung im Zusammenhang mit Personendaten. Neuerdings beschränkt sich das Recht auf informationelle Selbstbestimmung auf natürliche Personen. Auf den Schutz der Daten juristischer Personen soll, im Einklang mit den meisten ausländischen Rechtsordnungen, inskünftig verzichtet werden. Daher wird auch die Zweckbestimmung in Art. 1 E-DSG redaktionell geändert, indem ausdrücklich der Schutz auf natürliche Personen beschränkt wird.

[Rz 48] Diese Änderung hat keine Auswirkungen auf die Datenschutzbemühungen der Spitäler.

2.4.2. Geltungsbereich

[Rz 49] Der Anwendungsbereich wird leicht erweitert, was jedoch auf die Arbeit der Spitäler keine Auswirkungen hat.

[Rz 50] Es ist jedoch darauf hinzuweisen, dass das E-DSG genau wie das bisherige Recht das Datenschutzrecht im Allgemeinen regelt. Falls die Bearbeitung von Personendaten in den Anwendungsbereich anderer Bundesgesetze fällt, gelten aufgrund der Lex-specialis-Regel (besondere Normen gehen der allgemeinen Norm vor) grundsätzlich die bereichsspezifischen Datenschutznormen. Im Gesundheitswesen ist jedoch zu beachten, dass Bundesrecht kantonalem Recht immer vorgeht. Dies ist besonders bei der Herausgabe der Krankengeschichte gestützt auf das E-DSG zu beachten. So ist es rechtlich unerheblich, wenn kantonale Gesetze eine Kostenpflicht von Auskunftsbegehren statuieren,[37] das E-DSG jedoch eine Kostenlosigkeit vorschreibt.[38]

[Rz 51] Im Gegensatz zur EU-DSGVO enthält das E-DSG keine besondere Bestimmung zum räumlichen Geltungsbereich des Gesetzes. Für Schweizer Spitäler oder andere Leistungserbringer ist dies jedoch nicht von Relevanz. Für sie ist klar, dass sie entweder dem nationalen oder dem kantonalen Datenschutzgesetz unterstehen.

2.4.3. Begriffe

2.4.3.1. Personendaten

[Rz 52] Der Begriff der Personendaten wird im Vergleich zum bisherigen Recht leicht verändert, da das E-DSG auf juristische Personen nicht mehr anwendbar ist. Bei Personendaten handelt es sich somit um alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche (nicht mehr «oder juristische») Person beziehen (Art. 4 Bst. a E-DSG).

[Rz 53] Eine natürliche Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann.

[Rz 54] Die Identifizierung kann über eine einzige Information möglich sein (Krankenversicherungsnummer, AHV-Nummer, Fingerabdrücke) oder über den Abgleich verschiedener Informationen (Adresse, Geburtsdatum, Zivilstand oder IP-Adresse zusammen mit Daten des Providers[39]). Wie auch nach geltendem Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden, um eine Person zu identifizieren.

[Rz 55] Das Gesetz gilt also nicht für anonymisierte oder auch pseudonymisierte Daten, wenn eine Re-Identifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn dies nur mit einem hohen Aufwand möglich wäre, den kein Interessent auf sich nehmen würde.

[Rz 56] Die mit einem Schlüssel pseudonymisierten Daten im Besitz eines Dritten (ohne Schlüssel) gelten in Bezug auf diesen Dritten als anonymisiert. Anonymisierung zum weiteren Nutzen von Daten ist jedoch nicht immer zwingend zulässig. In Bezug auf medizinische Forschungsvor-

37 So z.B. Kanton ZH.

38 Siehe zu diesem Thema: Christian Peter, Wer trägt die Kosten für die Kopien der Krankengeschichte?, in: Jusletter 18. August 2014.

39 Vgl. Sachverhalt von BGE 136 II 508.

haben müssen weiterhin die Vorgaben des Humanforschungsgesetzes (HFG) beachtet werden. Dieses erlaubt die Anonymisierung der Daten und ihre anschliessende Nutzung für die Forschung am Menschen nur, wenn es sich nicht um biologisches Material oder genetische Personendaten handelt oder aber die betroffene Person vorgängig informiert wurde und sie nicht ihr Veto eingereicht hat (Art. 32 Abs. 3 HFG, Art. 30 der Humanforschungsverordnung; HFV).

2.4.3.2. Besonders schützenswerte Personendaten

[Rz 57] Unverändert gibt es die Gruppe der besonders schützenswerte Personendaten (Art. 4 Bst. c E-DSG). Der Begriff der besonders schützenswerten Personendaten wird in Einklang mit dem europäischen Recht auf die Daten zur ethnischen Herkunft sowie auf genetische Daten (Ziff. 3) und biometrische Daten, die ein Individuum eindeutig identifizieren (Ziff. 4), ausgeweitet.

[Rz 58] Biometrische Daten müssen jedoch zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt. Dies ist beispielsweise grundsätzlich nicht der Fall bei gewöhnlichen Fotografien.

2.4.3.3. Profiling

[Rz 59] Der alte Begriff «Persönlichkeitsprofil» soll aufgehoben und durch den Begriff des «Profiling» ersetzt werden (Art. 4 Bst. f E-DSG).

[Rz 60] Obwohl die beiden Begriffe Ähnlichkeiten aufweisen, sind sie nicht deckungsgleich. Das Persönlichkeitsprofil ist das Ergebnis eines Bearbeitungsprozesses und erfasst damit etwas Statisches. Das Profiling hingegen beschreibt einen dynamischen Prozess und erfasst nur noch die automatisierte Bearbeitung von Personendaten. Es ist definiert als die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Interessen, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen.

[Rz 61] Ein Profiling ist somit dadurch gekennzeichnet, dass Personendaten automatisiert ausgewertet werden, um auf der Grundlage dieser Auswertung, ebenfalls in automatisierter Weise, die Merkmale einer Person zu bewerten. Die umfangreichen Personalakten einer Mitarbeiterin konnten bisher als Persönlichkeitsprofil gelten. Das Bearbeiten dieser Daten stellt jedoch kein «Profiling» dar.

2.4.3.4. Verantwortlicher

[Rz 62] Das E-DSG ersetzt den Begriff «Inhaber der Datensammlung» durch «Verantwortlicher», um eine Einheitlichkeit mit dem europäischen Recht herbeizuführen.[40]

[Rz 63] Der Verantwortliche ist wie der Inhaber der Datensammlung derjenige, der über den Zweck und die Mittel (materielle oder automatisierte Bearbeitung, verwendete Software) der Bearbeitung entscheidet (Art. 4 Bst. i E-DSG). Hierbei handelt es sich wie bisher überwiegend um eine juristische Person; das Spital, eine Praxis, ein Heim oder die Spitex.

40 Siehe E-SEV 108 (Art. 2 Bst. d), in der Richtlinie (EU) 2016/680 (Art. 3 Ziff. 8) und in der Verordnung (EU) 2016/679 (Art. 4 Ziff. 7).

2.4.3.5. Auftragsbearbeiter

[Rz 64] Dabei handelt es sich um die Person, die im Auftrag des Verantwortlichen Daten bearbeitet. Der Auftragsbearbeiter ist ab dem Zeitpunkt, in dem er seine vertragliche Tätigkeit im Auftrag des Verantwortlichen beginnt, kein Dritter mehr.

[Rz 65] Zu denken ist an das Outsourcing oder den Bezug von IT-Dienstleistungen durch einen Informatikdienstanbieter.

2.4.3.6. Bearbeiten von Daten

[Rz 66] Aufgehoben wird der Begriff der «Datensammlung» stattdessen wird der Begriff «Bearbeiten[41] von Daten» verwendet. Diese Umbenennung wurde nötig, weil heute Daten nicht mehr zwingend zentral in einer Datenbank gespeichert werden müssen, um sie wie in einer solchen zu nutzen. So können zum Beispiel beim «Profiling» bestimmte Merkmale einer Person beurteilt werden, indem auf verschiedene Quellen zugegriffen wird, die keine Datensammlungen darstellen.

[Rz 67] Diese neue Terminologie führt dazu, dass die ursprüngliche Liste der Datensammlungen neu «Verzeichnis der Bearbeitungstätigkeit» heisst und zusätzlich diejenigen Bearbeitungen erfasst werden müssen, welche nicht auf einer Datensammlung beruhen (Art. 11 E-DSG).

2.4.4. Datenschutzgrundsätze

[Rz 68] Weiterhin von grosser Bedeutung sind die Datenschutzgrundsätze.

[Rz 69] Gemäss dem Grundsatz der Verhältnismässigkeit dürfen nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet und nötig sind. Die Grundsätze der Datenvermeidung und der Datensparsamkeit sind beide Ausdruck davon (Art. 5 Abs. 2 E-DSG).

[Rz 70] Diese beiden Grundsätze sind bereits bei der Planung neuer Systeme zu beachten. Somit überschneiden sie sich teilweise mit den Grundsätzen des Datenschutzes durch Technik (auch «privacy by design» genannt) und durch datenschutzfreundliche Voreinstellungen (sog. «privacy by default»).

[Rz 71] In Art. 5 Abs. 4 E-DSG wird nun explizit festgehalten, dass Daten vernichtet oder anonymisiert werden müssen, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

[Rz 72] Die Verpflichtung ergibt sich implizit auch aus dem allgemeinen Verhältnismässigkeitsgrundsatz, der in Abs. 2 der Bestimmung festgehalten ist. In Zeiten beinahe unbegrenzter Speichermöglichkeiten erschien es wichtig, diese Verpflichtung explizit festzuhalten.

[Rz 73] In Bezug auf die Behandlung von Patienten bedeutet dies, dass Patientendaten nach Ablauf der gesetzlichen Aufbewahrungsfrist vernichtet oder gelöscht werden müssen.

[Rz 74] Die Bestimmung zur Einwilligung der betroffenen Person in die Datenbearbeitung erfährt gewisse Retuschen (Art. 5 Abs. 6 E-DSG) doch erfolgt keine grundsätzliche Änderung der aktuellen Rechtslage. Wie bereits nach dem bestehenden Recht muss für eine gültige Einwilligung die Bearbeitung, insbesondere deren Umfang und Zweck, hinreichend bestimmt sein.

---

41 Das Schweizer Recht verwendet weiterhin den Begriff des «Bearbeitens». Dies obgleich die Europäische Union den Begriff des «Verarbeitens» nutzt. Inhaltlich bestehen keine Unterschiede.

[Rz 75] Gemäss dem Verhältnismässigkeitsgrundsatz muss die Zustimmung umso eindeutiger sein, je sensibler die fraglichen Personendaten sind. Die Einwilligung kann nach wie vor formfrei erfolgen und ist damit weiterhin nicht an eine schriftliche Erklärung gebunden (sie muss aber dokumentiert werden).

[Rz 76] Es muss mithin eine Willensäusserung erfolgen, sodass grundsätzlich blosses Schweigen oder Untätigkeit nicht als gültige Einwilligung in eine Persönlichkeitsverletzung gelten kann. Vorbehalten bleibt Art. 6 des Obligationenrechts (OR), wenn die Parteien «Schweigen» als Zustimmung vereinbart haben.

[Rz 77] Werden besonders schützenswerte Personendaten bearbeitet – wie dies bei der Patientenbehandlung immer der Fall ist – muss die Einwilligung ausdrücklich erfolgen (Art. 5 Abs. 6, 2. Satz E-DSG).

[Rz 78] «Ausdrücklich» ist eine erhöhte Anforderung an die «eindeutige» Einwilligung gemäss Satz 1 dieser Bestimmung. Die Tragweite dieser Anforderung ist bereits im aktuellen Recht unklar und daran ändert leider auch der Entwurf nichts.

[Rz 79] Eine Willenserklärung ist «ausdrücklich», wenn sie durch geschriebene oder gesprochene Worte oder ein Zeichen erfolgt und der geäusserte Willen aus den verwendeten Worten oder dem Zeichen unmittelbar hervorgeht. Die Willensäusserung als solche muss durch die Art und Weise, in der sie erfolgt, bereits Klarheit über den Willen schaffen. Dies ist insbesondere möglich durch das aktive Ankreuzen eines Kästchens oder anderweitige Erklärungen. Vorformulierten Einwilligungserklärungen, die bereits ein zustimmendes Häkchen enthalten, gelten nicht als gültige Einwilligungserklärung.

[Rz 80] Auch nonverbale Äusserung mittels eines im konkreten Kontext klaren Zeichens oder einer entsprechenden Bewegung, was namentlich im Rahmen eines ärztlichen Behandlungsverhältnisses häufig der Fall sein kann, gilt als «ausdrückliche» Zustimmung. Beispiele hierfür sind das zustimmende Kopfnicken oder das Öffnen des Mundes zur Entnahme von Wangenschleimhaut im Anschluss an die klare Aufklärung.

[Rz 81] Somit ist es weiterhin von zentraler Bedeutung, dass der Patient klar aufgeklärt wird und er seine Einwilligung zu einem eindeutigen Behandlungsplan erteilen kann.

2.4.5. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

[Rz 82] Art. 6 E-DSG führt die Pflicht zum Datenschutz durch Technik sowie durch datenschutzfreundliche Voreinstellungen ein. Weil diese Pflichten eng mit den Datenschutzgrundsätzen zusammenhängen, wurden sie in das Kapitel der allgemeinen Datenschutzbestimmungen überführt.

[Rz 83] Abs. 1 verlangt vom Verantwortlichen, ab dem Zeitpunkt der Planung eine Datenbearbeitung so auszugestalten, dass durch die getroffenen Vorkehren die Datenschutzvorschriften umgesetzt werden. Damit wird neu die Pflicht zum sogenannten «Datenschutz durch Technik» (Privacy by Design) eingeführt. Die Grundidee des technikgestützten Datenschutzes besteht darin, dass sich Technik und Recht gegenseitig ergänzen.

[Rz 84] Systeme zur Datenbearbeitung sollen technisch und organisatorisch so ausgestalten werden, dass sie insbesondere den Grundsätzen nach Art. 5 E-DSG entsprechen. Die gesetzlichen Anforderungen für eine datenschutzkonforme Bearbeitung werden mit anderen Worten bereits so im System verwirklicht, dass dieses die Gefahr von Verstössen gegen Datenschutzvorschriften

reduziert oder ausschliesst. Um dies zu erreichen, muss dem Datenschutz von Beginn eines jedes Projekts an die nötige Aufmerksamkeit geschenkt werden.

[Rz 85] So kann beispielsweise dafür gesorgt werden, dass Daten nach Ablauf der gesetzlichen Aufbewahrungspflicht in regelmässigen Abständen gelöscht werden oder dass mit einem Zugriffsmanagement die Zugriffe auf ein Klinikinformationssystem so vergeben werden, dass im Idealfall nur noch rechtmässige Zugriffe möglich sind.

[Rz 86] Besonders bedeutsam für den technikgestützten Datenschutz ist dabei die sogenannte Datenminimierung, welche sich bereits aus dem alten Recht und den allgemeinen Grundsätzen nach Art. 5 E-DSG ergibt. Eine Datenbearbeitung soll bereits von Beginn weg so angelegt werden, dass möglichst wenige Daten anfallen und bearbeitet werden oder dass Daten zumindest nur möglichst kurze Zeit aufbewahrt werden.

[Rz 87] Abs. 2 von Art. 6 E-DSG bringt zudem den risikobasierten Ansatz zum Ausdruck. Das Risiko, das mit einer Bearbeitung einhergeht, muss in Beziehung gesetzt werden zu den technischen Möglichkeiten, um dieses zu verringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können.

[Rz 88] Für Spitäler, Praxen, Heime und die Spitex bedeutet dies, dass ihre Technik im Einklang mit dem Umfang ihrer besonders schützenswerten Daten stehen muss. Je mehr besonders schützenswerte Patientendaten sie verarbeiten, umso höher muss der Stand der technischen Sicherheit sein.

[Rz 89] Die in Art. 6 Abs. 3 E-DSG statuierte Verpflichtung mittels geeigneter Voreinstellungen («Privacy by Default») soll dafür sorgen, dass grundsätzlich nur so wenig Personendaten bearbeitet werden, wie im Hinblick auf den Verwendungszweck nötig ist. Dies wird für diejenigen Spitäler wichtig, welche ihren Patienten z.B. Apps zur Verfügung stellen, mit welchen Gesundheitsdaten erhoben und für die Behandlung genutzt werden. Solche Apps müssen so voreingestellt sein, dass nur die für die Behandlung notwendigen Daten erhoben werden. Mittels Vereinbarung und Einstellungsänderungen durch den Betroffenen kann natürlich der Umfang der erhobenen und genutzten Daten erweitert werden.

[Rz 90] Für Spitäler, Praxen, Heime oder die Spitex bedeutet dies ganz allgemein, dass mit einem effektiven Zugriffsmanagement sichergestellt werden muss, dass möglichst nur rechtmässige Zugriffe technisch möglich sind. Weil dieser Idealzustand kaum erreicht werden kann, bedarf es neben den technischen Massnahmen auch noch organisatorische.

2.4.6. Datensicherheit

[Rz 91] Der Verantwortliche und der Auftragsbearbeiter müssen durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten (Art. 7 Abs. 2 E-DSG). Solche Massnahmen können, wie z.B. die Anonymisierung von Daten, sowohl dem Datenschutz (Art. 6) als auch der Datensicherheit (Art. 7 E-DSG) dienen.

2.4.7. Bearbeitung durch Auftragsbearbeiter

[Rz 92] In Art. 8 E-DSG wird der bisherige Art. 10a DSG übernommen.

[Rz 93] Für Spitäler, Praxen, Heimen und die Spitex ist wichtig zu wissen, dass nach wie vor das Berufsgeheimnis gemäss Art. 321 des Schweizerischen Strafgesetzbuches (StGB) der Bearbeitung durch einen Auftragsbearbeiter nicht entgegensteht, wenn der Auftragsbearbeiter als Hilfsperson im Sinne von Art. 321 Ziff. 1 Abs. 1 StGB qualifiziert werden kann. Somit ist die Auftragsbearbeitung zulässig, wenn die Voraussetzungen von Art. 8 E-DSG erfüllt sind (insb. der Auftragsbearbeiter die Daten so bearbeitet, wie der Verantwortliche es selbst tun dürfte) und es bedarf keiner zusätzlichen Einwilligung der betroffenen Person.[42]

[Rz 94] Abs. 3 von Art. 8 E-DSG ist neu und sieht vor, dass der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen darf. Im Privatsektor ist die Genehmigung an keine besondere Form gebunden, wird jedoch regelmässig in den Verträgen mit den Auftragsbearbeitern geregelt sein. Auf jeden Fall muss der Auftragsbearbeiter nachweisen können, dass die Genehmigung vorliegt.

[Rz 95] Werden Daten in einer von Dritten betriebenen Cloud aufbewahrt, handelt es sich dabei grundsätzlich um einen Anwendungsfall der Auftragsbearbeitung, welche die entsprechenden Voraussetzungen erfüllen muss. Falls hierfür Daten ins Ausland bekanntgegeben werden – was Spitäler nur mit verschlüsselten Daten tun dürfen oder mit Einwilligung der Betroffenen[43] müssen zudem die Voraussetzungen der Art. 13 und 14 E-DSG vorliegen.

2.4.8. Datenschutzberaterin oder -berater

[Rz 96] Art. 9 E-DSG regelt den betrieblichen Datenschutzberater. Das bisherige Recht verwendet den Begriff des Datenschutzverantwortlichen (Art. 11*a* Abs. 5 Bst. e DSG). Um Verwechslungen mit dem Verantwortlichen nach Art. 4 Bst. i E-DSG, zu vermeiden, führt das E-DSG den Begriff der Datenschutzberaterin und des Datenschutzberaters ein.

[Rz 97] Spitäler oder andere Leistungserbringer können – dies ist weiterhin freiwillig, aber mit gewissen Privilegien verbunden – einen Datenschutzberater ernennen, der die Einhaltung der Datenschutzvorschriften innerhalb eines Unternehmens überwacht und den Verantwortlichen in Datenschutzbelangen berät. Der Verantwortliche trägt jedoch allein die Verantwortung dafür, dass die Personendaten datenschutzkonform bearbeitet werden.

[Rz 98] Der Verantwortliche kann eine Mitarbeiterin oder einen Mitarbeiter oder eine Drittperson zur Datenschutzberaterin oder zum Datenschutzberater ernennen. Die Person muss ihre Funktion jedoch fachlich unabhängig ausüben können und darf gegenüber dem Verantwortlichen nicht weisungsgebunden sein (Art. 9 Abs. 2 Bst. a E-DSG). Grundsätzlich sollte sie oder er direkt der Geschäftsleitung des Verantwortlichen unterstellt sein.

[Rz 99] Die Unabhängigkeit des Datenschutzberaters wird weiter konkretisiert, indem er keine Tätigkeiten übernehmen darf, die mit seinen Aufgaben unvereinbar sind (Art. 9 Abs. 2 Bst. b E-DSG). So kann er nicht Mitglied der Geschäftsleitung sein, eine Funktionen in Bereichen der Personalführung oder der Informationssystemverwaltung ausüben oder zu einer Dienststel-

---

42 Botschaft zum E-DSG (Fn. 32), S. 7032; Christian Peter, Die Zulässigkeit der Auslagerung der Bearbeitung der Patientendaten von Spitälern an externe Informatikdienstleister, in: Jusletter 22. Juni 2009; Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, Nr. 1227 mit weiteren Hinweisen; a.A. Wolfgang Wohlers, Outsourcing durch Berufsgeheimnisträger, Patienten- und Mandantengeheimnisse als Schranke bei der Auslagerung von Datenverarbeitungen, digma 2016, S. 114 ff.

43 Um der Berufsgeheimnisnorm gemäss Art. 321 StGB zu genügen.

le gehören, die selbst besonders schützenswerte Personendaten bearbeitet. Hingegen ist es z. B. denkbar, die Aufgabe der Datenschutzberaterin zu kumulieren mit derjenigen der Informationssicherheitsbeauftragten. Schliesslich muss sie weiterhin über die erforderlichen Fachkenntnisse verfügen, um diese Aufgabe zu übernehmen. So ist für diese Tätigkeit Fachwissen im Bereich der Datenschutzgesetzgebung sowie über technischen Standards zur Datensicherheit erforderlich und sie muss den Betrieb selber in dem sie tätig ist, kennen.[44]

[Rz 100] Wurde ein Datenschutzberater ernannt und erfüllt er die an ihn gestellten Kriterien, muss der Datenschutzbeauftragte (EDÖB) im Rahmen einer Datenschutz-Folgenabschätzung[45] nicht konsultiert werden (Art. 21 Abs. 4 E-DSG).

2.4.9. Verhaltenskodizes

[Rz 101] Die Erarbeitung von Verhaltenskodizes soll gefördert werden (Art. 10 DSG). Es werden all diejenige von der Erstellung einer Datenschutz-Folgeabschätzung entbunden, welche einen Verhaltenskodex einhalten, der auf einer Datenschutz-Folgenabschätzung beruht, Massnahmen zum Schutz der Persönlichkeit der betroffenen Person vorsieht und dem Beauftragten vorgelegt wurde (Art. 20 Abs. 5 E-DSG).

[Rz 102] Solche Verhaltenskodizes können ausschliesslich von Berufs- und Wirtschaftsverbänden sowie den Bundesorganen erarbeitet werden. Diese können sie dem Datenschutzbeauftragten vorlegen, der dazu Stellung nimmt und die Stellungnahme veröffentlicht.

[Rz 103] Im Spitalumfeld ist vorstellbar, dass H+, Privatspitäler Schweiz, Curaviva oder SwissReha zusammen mit ihren Mitgliedern solche Verhaltenskodizes erarbeiten und dem EDÖB vorlegen.

2.4.10. Verzeichnis der Bearbeitungstätigkeiten

[Rz 104] Die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeit ersetzt die Meldepflicht von Datensammlungen nach dem bisherigen Recht (Art. 11 E-DSG). Die Verantwortlichen und Auftragsbearbeiter müssen ein Verzeichnis führen, welches Auskunft darüber erteilt, welche Daten sie wie bearbeiten (Bearbeitungszweck, Kategorie der Personendaten, Empfänger der Daten, Aufbewahrungsdauer etc.).

2.4.11. Zertifizierung

[Rz 105] Art. 12 E-DSG regelt die fakultative Zertifizierung, die gegenwärtig in Art. 11 DSG geregelt ist. Neben Datenbearbeitungssystemen (Verfahren, Organisation) und Produkten (Programme, Systeme) ist es künftig auch möglich, bestimmte Dienstleistungen zu zertifizieren.

---

44 Empfehlungen des EDÖB zum Betrieblichen Datenschutzverantwortlichen www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/betriebliche-datenschutzverantwortliche.html

45 Siehe hierzu hinten 2.4.14.2.

2.4.12. Datenbekanntgabe ins Ausland

[Rz 106] Der Grundsatz, wonach Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, wird aufgehoben. Neu ist die Bekanntgabe zulässig, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. (Art. 13 Abs. 1 E-DSG). Somit liegt neu ein gesetzlich verbindliches Kriterium für die Datenweitergabe vor, was zu mehr Rechtssicherheit führt. Liegt kein Entscheid des Bundesrates vor, müssen die in Art. 13 Abs. 2 E-DSG niedergeschriebenen Voraussetzungen erfüllt sein, um Daten weiterzuleiten. Schliesslich werden in Art. 14 E-DSG Ausnahmen definiert und in Art. 15 E-DSG wird festgehalten, dass die Veröffentlichung von Personendaten im Internet zwecks Information der Öffentlichkeit nicht als Bekanntgabe von Personendaten ins Ausland zu betrachten ist.

[Rz 107] Für Spitäler, Praxen, Heime oder die Spitex sind die Bestimmungen des Datenschutzgesetzes für die Datenweitergabe ins Ausland nicht der limitierende Faktor. Vielmehr ist dies das Berufsgeheimnis nach Art. 321 StGB. Dieses lässt eine Weitergabe der Patientendaten ins Ausland nur zu, wenn die betroffenen Personen eingewilligt und somit auf den Schutz des Berufsgeheimnisses verzichtet haben.[46]

2.4.13. Daten von Verstorbenen

[Rz 108] Neben der Einsicht in die Daten einer verstorbenen Person wird ein Recht auf Löschung bzw. Vernichtung der Daten des Verstorbenen durch die Erben eingeführt. Der «digitale Tod» soll herbeigeführt werden können.

[Rz 109] Gemäss Art. 16 Abs. 1 E-DSG hat der Verantwortliche kostenlos Einsicht in die Daten einer verstorbenen Person zu gewähren, wenn kumulativ die drei Voraussetzungen erfüllt sind:

a. ein schutzwürdiges Interesse an der Einsicht vorliegt oder die Person, die Einsicht verlangt, mit der verstorbenen Person in gerader Linie verwandt ist, mit ihr bis zum Zeitpunkt des Todes verheiratet war, in eingetragener Partnerschaft lebte oder eine faktische Lebensgemeinschaft führte oder wenn sie ihr Willensvollstrecker ist;
b. der Einsicht weder eine ausdrückliche Erklärung (z.B. in einem Testament) noch ein besonderes Schutzbedürfnis der verstorbenen Person entgegenstehen und
c. keine überwiegenden Interessen des Verantwortlichen oder von Dritten der Einsicht entgegenstehen.

[Rz 110] Steht eine Berufsgeheimnispflicht wie das Berufsgeheimnis gemäss Art. 321 StGB der Einsichtnahme in die Patientendaten entgegen, stellt Art. 16 E-DSG ein Rechtfertigungsgrund für die Datenbekanntgabe dar. In einem solchen Fall stellt die Offenbarung eine rechtmässige Handlung im Sinne von Art. 14 StGB dar und der Geheimnisträger kann nicht wegen Verletzung des Amts- oder Berufsgeheimnisses bestraft werden.

[Rz 111] Zu denken ist beispielsweise an den Sohn einer Verstorbenen, der beim Spital Einsicht in die medizinischen Daten seiner verstorbenen Mutter verlangt. Zwar gilt die strafrechtliche

46 Ursula Widmer, Gesundheitsdaten in der Cloud, in: P. Schartner / J. Taeger (Hrsg.) / DACH Security 2011 / syssec (2011), S. 170; Christian Peter, a.a.O. (Fn. 41).

Schweigepflicht für Amts- und Berufsgeheimnisträger auch über den Tod des Geheimnisherrn hinaus, weshalb Geheimnisträger grundsätzlich nicht zur Offenbarung verpflichtet werden können. Mit der neuen Bestimmung dürfen sie nun Einsicht oder Auskunft in die Krankengeschichte des Verstorbenen gewähren, müssen es jedoch nicht. Eine Entbindung von der Aufsichtsbehörde, um den Hinterbliebenen umfassende Einsicht oder Auskunft zu erteilen, ist somit nicht mehr nötig.

[Rz 112] Verweigert ein Spital die Einsicht unter Hinweis auf ein Amts- oder Berufsgeheimnis, so kann eine Person, die mit einer verstorbenen Person in gerader Linie verwandt ist, mit ihr bis zum Zeitpunkt des Todes verheiratet war, in eingetragener Partnerschaft lebte, eine faktische Lebensgemeinschaft führte oder ein schutzwürdiges Interesse an der Einsicht geltend macht die zuständige kantonale Gesundheitsbehörde um Entbindung des Verantwortlichen von seiner Geheimhaltungspflicht ersuchen. Dies ist eine Ausnahme vom Grundsatz, dass lediglich der Geheimnisträger an die Aufsichtsbehörde zur Entbindung von der Berufsgeheimnispflicht gelangen kann.

[Rz 113] Dies stellt für Spitäler, Praxen, Heime und die Spitex eine administrative Entlastung in den Fällen dar, in welchen sie mit Bitten um Einsicht in die Behandlungsunterlagen eines Verstorbenen durch Hinterbliebene konfrontiert sind. Neu können sie, wenn die Voraussetzungen von Art. 16 E-DSG erfüllt sind, ohne ein Gesuch um Entbindung von der Berufsgeheimnispflicht an die Aufsichtsbehörde Einsicht in die Behandlungsunterlagen gewähren. Sehen sie die Voraussetzungen nicht als erfüllt an oder wollen sie die Einsicht aus anderen Gründen nicht gewähren, ist es an dem Einsichtswilligen, ein Gesuch zu stellen.

[Rz 114] Das neu statuierte Recht der Erben, die Vernichtung der Daten des Verstorbenen zu verlangen, wird durch ein mögliches überwiegendes öffentliches Interesse eingeschränkt (Art. 16 Abs. 3 E-DSG). Zu denken ist an Aufbewahrungspflichten nach Massgabe des Bundesrechts[47] oder des kantonalen Rechts[48].

2.4.14. Pflichten des Verantwortlichen und des Auftragsbearbeiters

2.4.14.1. Informationspflicht

[Rz 115] In Art. 17 E-DSG wird neu die Informationspflicht bei der Beschaffung von Daten geregelt. Die Informationspflicht verbessert die Transparenz bei der Datenbearbeitung. Das E-DSG legt nicht fest, auf welche Weise die Information erfolgen muss. Der Verantwortliche muss aber sicherstellen, dass die betroffene Person die Information tatsächlich zur Kenntnis nehmen kann. So kann eine allgemeine Information genügen, wenn die Personendaten bei der betroffenen Person beschafft werden (zu allgemeinen Geschäftsbedingungen vgl. Art. 18 Abs. 1 E-DSG). Denkbar sind in diesem Fall eine Datenschutzerklärung auf einer Website, aber gegebenenfalls auch Symbole oder Piktogramme, soweit sie die nötigen Informationen wiedergeben.

47 Art. 19 Abs. 3 der Verordnung über mikrobiologische Laboratorien vom 29. April 2015 (SR 818.101.32) oder Art. 40 des Bundesgesetzes über Arzneimittel und Medizinprodukte vom 15. Dezember 2000 (HMG; SR 812.21).

48 BE: Art. 26 Abs. 1 des Gesundheitsgesetzes des Kantons Berns vom 2. Dezember 1984 (GesG; BSG 811.01); ZH: Art. 13 Abs. 3 des Gesundheitsgesetzes des Kantons Zürich vom 2. April 2007 (GesG; LS 810.1); LU: § 26 Abs. 2 des Gesundheitsgesetzes des Kantons Luzerns vom 13. September 2005 (GesG; SRL 800); AG: § 15 des Gesundheitsgesetzes des Kantons Aargau vom 20. Januar 2009 (GesG; AGS 301.100).

[Rz 116] Werden die Daten hingegen nicht bei der betroffenen Person beschafft, muss der Verantwortliche prüfen, wie die Information erfolgen muss, damit die betroffene Person tatsächlich von ihr Kenntnis nehmen kann. Gegebenenfalls reicht es in diesem Fall nicht aus, lediglich Informationen zur Verfügung zu stellen, sondern die betroffene Person muss aktiv informiert werden.

[Rz 117] Art. 18 E-DSG regelt, unter welchen Umständen die Informationspflicht gänzlich entfällt (Abs. 1 und 2), und wann die Information eingeschränkt werden kann, obschon grundsätzlich die Pflicht zur Information besteht (Abs. 3).

[Rz 118] In den Spitälern, Praxen, Heimen und der Spitex werden die Informationen immer mit der Einwilligung des Patienten, der die Informationen in der Regel selber erteilt oder in die Datenweitergabe vom Zuweisenden an das Spital einwilligt, bearbeitet und folglich führen diese Bestimmungen zu keinen neuen Herausforderungen.

2.4.14.2. Datenschutz-Folgenabschätzung

[Rz 119] Art. 20 E-DSG führt neu die Pflicht zum Erstellen einer Datenschutz-Folgenabschätzung ein. Damit fällt ein datenschutzrechtliches Privileg der dem nationalen Datenschutzrecht unterstehenden Organisationen gegenüber den dem kantonalen Recht unterstehenden. Letztere mussten sich schon seit langem einer mit der Datenschutz-Folgenabschätzung vergleichbaren Vorabkontrolle unterziehen, wenn eine automatisierte Personendatenverarbeitung eingeführt werden sollte.[49]

[Rz 120] Eine Datenschutz-Folgenabschätzung ist ein Instrument, um Risiken zu erkennen und zu bewerten, welche für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis dieser Abschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen. Eine solche Abschätzung ist daher auch für den Verantwortlichen vorteilhaft, weil sie ihm erlaubt, allfällige datenschutzrechtliche Probleme präventiv anzugehen und dadurch nicht zuletzt Kosten zu sparen.

2.4.14.2.1. Gründe für eine Datenschutz-Folgenabschätzung

[Rz 121] Nach Art. 20 Abs. 1 E-DSG muss ein Spital oder ein anderer Leistungserbringer vorgängig eine Datenschutz-Folgenabschätzung durchführen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit der betroffenen Person führt.

[Rz 122] Die Höhe des Risikos ergibt sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Je umfangreicher die Bearbeitung, je sensibler die bearbeiteten Daten, je umfassender der Bearbeitungszweck, umso eher ist ein hohes Risiko anzunehmen.

[Rz 123] Nach Art. 20 Abs. 2 Bst. a E-DSG liegt ein hohes Risiko vor, wenn in umfangreicher Form besonders schützenswerte Personendaten bearbeitet werden, wie dies beispielsweise bei medizinischen Forschungsprojekten der Fall sein kann oder bei einem Klinikinformationssystem.

---

49 Vgl. Art.17a des Datenschutzgesetzes des Kantons Berns vom 19. Februar 1986 (KDSG; BSG 152.040.1) oder § 23 des Gesetzes über den Schutz von Personendaten des Kanton Luzerns vom 2. Juli 1990 (Datenschutzgesetz, DSG; SRL 38).

[Rz 124] Bei der Konkretisierung dieses Risikos stehen das Recht auf informationelle Selbstbestimmung sowie das Recht auf Privatsphäre im Vordergrund. Diese schützen sowohl die Autonomie des Einzelnen als auch dessen Würde und Identität.

[Rz 125] Die Datenschutz-Folgenabschätzung muss eine Beschreibung der geplanten Bearbeitung enthalten (Art. 20 Abs. 3 E-DSG). So müssen beispielsweise die verschiedenen Bearbeitungsvorgänge (z. B. die verwendete Technologie), der Zweck der Bearbeitung oder die Aufbewahrungsdauer aufgeführt werden. Im Weiteren muss aufgezeigt werden, welche Risiken für die Persönlichkeit der betroffenen Person die fraglichen Bearbeitungsvorgänge mit sich bringen können. Es handelt sich hier um eine Vertiefung der Risikobewertung, die bereits im Hinblick auf die Notwendigkeit einer Datenschutz-Folgenabschätzung vorzunehmen ist.

[Rz 126] Schliesslich muss in der Datenschutz-Folgenabschätzung erläutert werden, mit welchen Massnahmen diese Risiken bewältigt werden sollen. Massgebend dafür sind insbesondere die Grundsätze nach Art. 5 E-DSG[50], aber auch die Pflicht zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen (privacy by design resp. privacy by default, Art. 6 E-DSG) können relevant sein. Bei diesen Massnahmen darf auch eine Abwägung zwischen den Interessen der betroffenen Personen und denjenigen des Verantwortlichen erfolgen. Diese Interessenabwägung ist in der Datenschutz-Folgenabschätzung ebenfalls aufzuführen und entsprechend zu begründen.

[Rz 127] Für Spitäler, Praxen, Heime oder für die Spitex bedeutet dies, dass in Zukunft vor Inbetriebnahme von neuen Klinikinformations-, ERP- oder anderen IT-Lösungen, mit welchen im grossen Umfang besonders schützenswerte Personendaten bearbeitet werden, eine Datenschutz-Folgeabschätzung durchgeführt werden muss.

2.4.14.2.2Ausnahmen von der Datenschutz-Folgeabschätzung

[Rz 128] Keine Datenschutz-Folgenabschätzung müssen Organisationen machen, die Daten in Erfüllung einer gesetzlichen Pflicht bearbeiten. Dabei ist beispielsweise an die Bearbeitung von Daten zur Bekämpfung von Terrorismus oder Geldwäscherei zu denken. Werden Daten aufgrund einer gesetzlichen Verpflichtung lediglich für solche Zwecke bearbeitet, ist davon auszugehen, dass der Gesetzgeber allfällige Risiken für die betroffene Person im Vergleich zum Bearbeitungszweck abgewogen und gegebenenfalls entsprechende Vorschriften erlassen hat (Art. 20 Abs. 4 E-DSG).

[Rz 129] Nicht ausgenommen sind hingegen Bearbeitungen, die nicht ausschliesslich zur Erfüllung einer gesetzlichen Pflicht erfolgen. Hierfür muss eine Datenschutz-Folgenabschätzung erstellt werden. Die Dokumentierung der Behandlung erfolgt z.B. nicht ausschliesslich zur Erfüllung einer gesetzlichen Pflicht. Dokumentiert wird in erster Linie für die Behandlung. Daher können sich Spitäler, Praxen, Heime und die Spitex nicht auf diese Ausnahme berufen, um eine Datenschutz-Folgeabschätzung bei der Einführung einer Datenbearbeitung zu umgehen.

---

50 Rechtmässigkeit der Beschaffung, Bearbeitung nach Treu und Glauben und zweckgebunden, Verhältnismässigkeit, Richtigkeit.

[Rz 130] Sie können jedoch von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn sie sich für die fragliche Bearbeitung einer Zertifizierung nach Art. 12 unterzogen haben oder wenn sie einen Verhaltenskodex[51] gemäss Art. 10 E-DSG erfüllen (Art. 20 Abs. 5 E-DSG).

2.4.14.2.3 Konsultation des EDÖBs

[Rz 131] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hätte, wenn der Verantwortliche keine Massnahmen träfe, so hat er vorgängig die Stellungnahme des Datenschutzbeauftragten einzuholen (Art. 21 Abs. 1 E-DSG). Der EDÖB hat anschliessend zwei Monate Zeit, um dem Verantwortlichen seine Einwände gegen die geplante Bearbeitung mitzuteilen.[52]

2.4.14.2.4 Ausnahme von der Konsultation des EDÖBs

[Rz 132] Der Verantwortliche kann von der Konsultation des EDÖBs absehen, wenn er einen qualifizierten Datenschutzberater eingesetzt und diesen in Bezug auf die Datenschutz-Folgenabschätzung konsultiert hat (Art. 21 Abs. 4 E-DSG). Der Datenschutzberater muss sich tatsächlich mit der Datenschutz-Folgenabschätzung auseinandergesetzt haben. Das heisst, es reicht für die Privilegierung nicht aus, dass der Verantwortliche lediglich einen Datenschutzberater ernennt. Vielmehr muss dieser aktiv in die Erarbeitung der Datenschutz-Folgenabschätzung involviert sein.

[Rz 133] Die Bestimmung soll Unternehmen entlasten und ihnen zugleich einen Anreiz geben, einen Datenschutzberater einzusetzen.

2.4.14.3. Meldung von Verletzungen der Datensicherheit

[Rz 134] Art. 22 E-DSG führt die Pflicht zur Meldung von Verletzungen der Datensicherheit ein.

[Rz 135] Nach Abs.1 hat das Spital oder andere Leistungserbringer[53] dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit der betroffenen Person führt, zu melden. Unbedeutende Verletzungen müssen nicht gemeldet werden.

[Rz 136] Gemäss Art. 4 Bst. g E-DSG handelt es sich um eine Verletzung der Sicherheit, die, ungeachtet der Absicht oder der Widerrechtlichkeit, dazu führt, dass Personendaten verloren gehen, gelöscht oder vernichtet, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden.

[Rz 137] Irrelevant für das Vorliegen einer Verletzung der Datensicherheit ist ebenfalls, ob lediglich die Möglichkeit bestand, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht wurden, oder ob ein solcher Zugang tatsächlich stattgefunden hat. Geht beispielsweise

51 Siehe vorne 2.4.9.

52 Diese Frist kann um einen Monat verlängert werden, wenn es sich um eine komplexe Datenbearbeitung handelt (Art. 21 Abs. 2 E-DSG).

53 Eine Verletzung der Datensicherheit kann auch beim Auftragsbearbeiter auftreten. Daher ist dieser nach Abs. 3 verpflichtet, dem Verantwortlichen so rasch als möglich jede unbefugte Datenbearbeitung zu melden.

ein Datenträger verloren, lässt sich oft kaum nachweisen, ob die darauf gespeicherten Daten tatsächlich durch Unbefugte eingesehen oder verwendet wurden. Daher stellt bereits der Verlust als solches eine Verletzung der Datensicherheit dar.

[Rz 138] Da auf eine Gefährdung ihrer eigenen Daten eine betroffene Person nur reagieren kann, wenn sie von der Verletzung der Datensicherheit weiss, muss der Verantwortliche prinzipiell eine unbefugte Bearbeitung melden, wobei die Meldung zunächst an den EDÖB geht und nur, wenn es zum Schutz der betroffenen Person erforderlich ist an die betroffene Person (Art. 22 Abs. 4 E-DSG). Bedeutsam ist insbesondere, ob durch die Information die Risiken für die Persönlichkeit der betroffenen Person reduziert werden können.

[Rz 139] Dies ist insbesondere der Fall, wenn die betroffene Person entsprechende Vorkehren zu ihrem Schutz treffen muss, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändert.

[Rz 140] Bei Patientendaten eines Spitals, einer Praxis, eines Heims oder der Spitex, auf welche die Patientinnen und Patienten keinen direkten Zugriff haben, ist es nur schwer vorstellbar, dass eine Benachrichtigung an die betroffene Person nötig wird. Anders kann es beim elektronischen Patientendossier gemäss des Bundesgesetzes über das elektronische Patientendossier (EPDG) aussehen. Gehen Zugangsdaten der Nutzer bei einer Gemeinschaft verloren, müsste diese seine Kunden informieren.

[Rz 141] Der Verantwortliche kann nach Art. 22 Abs. 5 E-DSG die Information an die betroffenen Personen einschränken, aufschieben oder darauf verzichten, wenn einer der Gründe von Art. 24 Abs. 1 Bst. b oder Abs. 2 Bst. b E-DSG vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet. Zudem wenn die Information unmöglich ist. Dies ist der Fall, wenn der Verantwortliche gar nicht weiss, welche Personen von der Verletzung der Datensicherheit betroffen sind, beispielsweise weil die Logfiles, aus denen dies ersichtlich wäre, nicht mehr vorhanden sind. Auch bei einem unverhältnismässigen Aufwand kann auf die Information der betroffenen Personen verzichtet werden. Ein unverhältnismässiger Aufwand würde beispielsweise vorliegen, wenn bei einer grossen Anzahl Betroffener diese einzeln informiert werden müssten und die dadurch verursachten Kosten im Verhältnis zum Informationsgewinn für die betroffene Person unverhältnismässig erschienen.

2.4.15. Recht der Betroffenen

2.4.15.1. Auskunftsrecht

[Rz 142] Das Auskunftsrecht ergänzt die Informationspflicht des Verantwortlichen und bildet die zentrale Grundlage dafür, dass die betroffene Person ihre Rechte nach diesem Gesetz überhaupt wahrnehmen kann. Das Auskunftsrecht ist ein subjektives, höchstpersönliches Recht, das auch urteilsfähige handlungsunfähige Personen selbständig, ohne Zustimmung ihres gesetzlichen Vertreters, geltend machen können (z.B. urteilsfähige Jugendliche, die noch nicht 18 Jahre alt sind). Aus dem Charakter des höchstpersönlichen Rechts ergibt sich auch, dass niemand im Voraus auf das Auskunftsrecht verzichten kann (Art. 23 Abs. 5 E-DSG).

[Rz 143] Nach Abs. 1 kann jede Person vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

[Rz 144] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist (Art. 23 Abs. 2 E-DSG). Die in Art. 24 Abs. 2 E-DSG nicht abschliessende Auf-

zählung erfasst grundsätzlich sämtliche Informationen, die der Verantwortliche der betroffenen Person mitteilen muss. Subsidiär erlaubt die Generalklausel im Einleitungssatz, gegebenenfalls weitere Informationen zu verlangen, wenn diese für die betroffene Person erforderlich sind, um ihre Rechte nach diesem Gesetz geltend zu machen und eine transparente Datenbearbeitung zu gewährleisten. Wenn er grosse Datenmengen über die betroffene Person bearbeitet, kann der Auskunftspflichtige gegebenenfalls verlangen, dass die betroffene Person präzisiert, auf welche Informationen oder welche Bearbeitungsvorgänge sich ihr Auskunftsgesuch bezieht. Die Präzisierung erfolgt vor dem Hintergrund der zahlreichen Stellungnahmen in der Vernehmlassung sowie in der Lehre, die kritisieren, dass das Auskunftsrecht häufig zu anderen, datenschutzfremden Zwecken verwendet werde. Angesprochen sind insbesondere Fälle, in denen das Auskunftsrecht ausschliesslich zur Beschaffung von Beweismitteln für Zivilprozesse benutzt wird, die in keinem Zusammenhang mit dem Datenschutz stehen.

[Rz 145] Besonders gestützt auf die Generalklausel steht es den Patientinnen und Patienten eines Spitals zu, Auskunft über das ganze Behandlungsdossier zu verlangen. Auskunft bedeutet, dass ein Patient in schriftlicher Form erfährt, welche Daten über ihn bearbeitet werden. Konkret heisst das, dass er Kopien sämtlicher ihn betreffenden Unterlagen erhalten muss.

[Rz 146] Aus dem geltenden Recht unverändert übernommen wurde Abs. 3, wonach der Verantwortliche Informationen über die Gesundheit der betroffenen Person durch eine von dieser bezeichneten Gesundheitsfachperson mitteilen lassen kann. Die Gesundheitsfachperson muss die Qualifikationen haben, die im fraglichen Fall erforderlich sind, muss jedoch nicht wie noch im geltenden Recht[54] ein Arzt sein.

[Rz 147] Der Bundesrat kann Ausnahmen von der Kostenlosigkeit vorsehen (Art. 23 Abs. 6 E-DSG).

2.4.15.2. Einschränkungen des Auskunftsrechts

[Rz 148] Art. 24 E-DSG regelt die Einschränkungen des Auskunftsrechts. Sie wurden mit wenigen redaktionellen Anpassungen unverändert aus dem bisherigen Recht übernommen.

[Rz 149] Der Verantwortliche kann die Auskunft verweigern, einschränken oder aufschieben, wenn ein Gesetz im formellen Sinn dies vorsieht und es aufgrund überwiegender Interessen Dritter erforderlich ist. Neu ist, dass ein Auskunftsrecht auch eingeschränkt werden kann, wenn das Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist (Art. 24 Abs. 1 E-DSG).

[Rz 150] Wir die Auskunft verweigert, eingeschränkt oder aufgeschoben, muss dies begründet und mitgeteilt werden.

2.4.16. Besondere Bestimmungen zur Datenbearbeitung durch private Personen

2.4.16.1. Persönlichkeitsverletzungen

[Rz 151] Die Vorschriften zum Bearbeiten von Personendaten durch private Personen konkretisieren den Schutz der Persönlichkeit nach Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB) in Bezug auf den Datenschutz und dienen damit der Verwirklichung der informationellen Selbstbestimmung unter Privaten.

54 Art. 8 Abs. 3 DSG.

[Rz 152] Der vorliegende Entwurf behält die bestehende Regelung weitgehend bei. Die Bearbeitung der Personendaten darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Eine solche liegt insbesondere vor, wenn Personendaten entgegen den Grundsätzen nach Art. 5 (Datenschutzgrundsätze) und Art. 7 E-DSG (Datensicherheit) bearbeitet werden oder Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden und Dritten besonders schützenswerte Personendaten bekanntgegeben werden.

2.4.16.2. Rechtfertigungsgründe

[Rz 153] Gemäss Art. 27 Abs. 2 E-DSG kann eine Persönlichkeitsverletzung gerechtfertigt werden, wenn sie durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

[Rz 154] Da bei der Bearbeitung von Patientendaten jeweils eine Einwilligung in die Behandlung vorliegt und somit auch in die Bearbeitung der Daten zum Zweck der Behandlung, ist die Datenbearbeitung gerechtfertigt, wenn sie sich an die Grundsätze von Art. 5 und 7 E-DSG hält.

[Rz 155] Leicht verschärft wird der Rechtfertigungsgrund der Bearbeitung zu nicht personenbezogenen Zwecken, insbesondere in der Forschung, Planung oder Statistik (Art. 27 Abs. 2 Bst e E-DSG). Die Verwendung von Daten zu diesen Zwecken ist neu nur zulässig, wenn die Voraussetzungen der Ziffern 1–3 erfüllt sind. Durch diese Regelung soll der Schutz besonders schützenswerter Personendaten verstärkt werden. Dies erfolgt insbesondere mit Blick auf die Möglichkeiten von Big Data und die zunehmende Digitalisierung des Alltags, die auch dazu führt, dass eine immer grössere Anzahl besonders schützenswerter Personendaten bearbeitet wird.

[Rz 156] Folgenden Voraussetzungen müssen erfüllt sein:

1. Die Daten werden anonymisiert[55], sobald der Bearbeitungszweck es erlaubt.
2. Besonders schützenswerte Personendaten werden Dritten so bekanntgegeben, dass die betroffenen Personen nicht bestimmbar sind.
3. Die Ergebnisse werden so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind.

2.4.17. Rechtsansprüche der betroffenen Person

[Rz 157] Art. 28 E-DSG definiert die Rechtsansprüche der betroffenen Person.

[Rz 158] Unabhängig von einer Persönlichkeitsverletzung nach Art. 26 E-DSG kann jede Person die Berichtigung unrichtiger Personendaten verlangen.

[Rz 159] Die Berichtigung unrichtiger Daten ist nur ausgeschlossen, wenn eine gesetzliche Vorschrift die Änderung der Personendaten ausschliesst (Art. 28 Abs. 1 Bst a E-DSG). Zu denken ist hierbei an gesetzliche Bearbeitungs- und Aufbewahrungspflichten, nach denen Verantwortliche Daten unverändert belassen müssen.

[Rz 160] Art. 28 Abs. 2 E-DSG enthält den Verweis auf die Klagen nach Art. 28 ff. ZGB, welcher bereits im bisherigen Recht besteht. Die klagende Partei kann insbesondere verlangen, dass eine

55 Diese Voraussetzung ist ebenfalls erfüllt, wenn die Weitergabe in pseudonymisierter Form erfolgt und der Schlüssel bei der weitergebenden Person verbleibt (faktische Anonymisierung).

bestimmte Datenbearbeitung verboten wird, eine bestimmte Bekanntgabe von Personendaten an Dritte untersagt wird oder dass Personendaten gelöscht resp. vernichtet werden.

[Rz 161] Das Recht auf Löschung entspricht im Bereich des Datenschutzes dem «Recht auf Vergessenwerden», wie es generell aus dem zivilrechtlichen Persönlichkeitsschutz abgeleitet wird. Ein solches Recht gilt indessen nicht absolut. Vielmehr wird in der Rechtsprechung zum Persönlichkeitsschutz grundsätzlich das Interesse der betroffenen Person abgewogen gegen die Meinungs- und Informationsfreiheit, aus der sich regelmässig ein überwiegendes Interesse am Fortbestehen bzw. an der Verwendung der Information ergibt. Ein solches Interesse kann beispielsweise bestehen bei Archiven oder Bibliotheken, deren Aufgabe es ist, Dokumente unverändert zu sammeln, zu erschliessen, zu erhalten und zu vermitteln.

[Rz 162] In Art. 28 Abs. 3 E-DSG wird der so genannte Bestreitungsvermerk behandelt, der unverändert aus dem bisherigen Recht übernommen wird und z.B. dann zur Anwendung kommt, wenn eine Person die Richtigkeit einer Diagnose im Behandlungsdossier bestreitet. In solchen Fällen wird im Behandlungsdossier nicht die Diagnose geändert, sondern festgehalten, dass der Patient die Korrektheit der Diagnose bestreitet.

[Rz 163] In Art. 28 Abs. 4 E-DSG wird schliesslich – wie im bisherige Recht – festgehalten, dass die klagende Partei verlangen kann, dass die Berichtigung, die Löschung oder die Vernichtung, das Verbot der Bearbeitung oder der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

2.4.18. Untersuchung von Verstössen gegen Datenschutzvorschriften

[Rz 164] Gemäss Art. 43 Abs. 1 E-DSG eröffnet der Datenschutzbeauftragte von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Die Anzeige kann nicht nur durch die betroffene Person erfolgen, sondern auch durch einen Dritten; dies im Gegensatz zur Anzeige einer Berufsgeheimnisverletzung gemäss Art. 321 StGB.[56]

[Rz 165] Er kann von der Eröffnung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist. Das wäre etwa der Fall, wenn ein Fussballverein allen seinen Mitgliedern eine E-Mail-Nachricht sendet, ohne die Identität der Empfängerinnen und Empfänger zu verbergen.

2.4.19. Strafbestimmungen

[Rz 166] Trotz grosser Kritik in der Vernehmlassung, dass die Strafbestimmungen einzelne Personen des Unternehmens treffen und nicht das Unternehmen selber, liess sich der Bundesrat von diesem Systementscheid nicht abbringen.[57] Da die Geldstrafen auf natürliche Personen zielen und nicht auf Unternehmen, sind sie im Vergleich zu den Bussen im europäischen Recht auch markant tiefer.

---

56 Art. 321 StGB ist ein Antragsdelikt und der Antrag muss durch das Opfer gestellt werden.

57 Die Kritiker wünschten sich, dass Unternehmen über Verwaltungssanktionen des Datenschutzbeauftragten (oder einer zu diesem Zweck geschaffenen Kommission) sanktioniert würden.

[Rz 167] Das Fehlen von ernsthaften direkten Sanktionen für Datenschutzverstösse für ein Unternehmen hat sicherlich Einfluss auf die Priorisierung des Datenschutzes in der Privatwirtschaft.[58] In wie fern dies auch auf Spitäler, Praxen, Heime oder die Spitex zutrifft, ist unklar. Aufgrund des Umstands, dass die Einhaltung des Datenschutzes und des Berufsgeheimnisses für die Reputation der Dienstleister im Gesundheitswesen ein wichtiges Element ist, ist zu hoffen, dass Spitäler, Praxen, Heime und die Spitex den Datenschutz sehr hoch priorisieren.

2.4.19.1. Adressat der Strafbestimmungen

[Rz 168] Die Strafbestimmungen zielen weiterhin auf Leitungspersonen, welche als Organ oder als Mitglied eines Organs der Organisation oder als Mitarbeiter mit selbständigen Entscheidungsbefugnissen in seinem Tätigkeitsbereich handelt (Art. 29 StGB und Art. 6 des Bundesgesetzes über das Verwaltungsstrafrecht; VStrR).

[Rz 169] Es muss sich somit um Personen handeln, welche eine Garantenstellung für die Einhaltung der Rechtspflicht haben. Das heisst, es liegt an ihnen, das fragliche Verhalten durch Überwachung, Weisungen und falls notwendig Eingreifen zu verhindern.[59]

[Rz 170] Die in der Vernehmlassung geäusserte Sorge, dass jeder beliebige Angestellte eines Unternehmens bestraft werden könnte, erweist sich deshalb als unbegründet.

2.4.19.2. Verletzung der Sorgfaltspflicht

[Rz 171] Die Sanktionierung von Verletzungen der Sorgfaltspflicht ist neu. Sie ist notwendig, weil das E-DSG neue elementare Pflichten vorsieht, die von den geltenden Strafbestimmungen nicht abgedeckt werden. Ein wirksamer Schutz der Persönlichkeit der betroffenen Personen ist dann möglich, wenn die Verantwortlichen und die Auftragsbearbeiter ihren Pflichten gerecht werden.

[Rz 172] Gemäss Art 55 E-DSG wird auf Antrag mit Busse bis zu CHF 250'000 bestraft, wer vorsätzlich (das heisst mit Wissen und Willen) Daten unrechtmässig ins Ausland bekannt gibt, die Datenbearbeitung unerlaubterweise einem Auftragsbearbeiter übergibt oder die Mindestanforderungen an die Datensicherheit nicht einhält.

[Rz 173] Auf die Pönalisierung von fahrlässigen Pflichtverletzungen wird verzichtet.

2.4.19.3. Verletzung der beruflichen Schweigepflicht

[Rz 174] Mit der Strafbestimmung von Art 56 E-DSG wird der eingeschränkte Täterkreis der Art. 320 (Amtsgeheimnis) und 321 StGB (Berufsgeheimnis) erweitert. Er sieht eine Schweigepflicht auch für Personen vor, die nicht unter Art. 320 oder 321 StGB fallen.

[Rz 175] Wer geheime Personendaten – diese müssen nicht besonders schützenswert sein – vorsätzlich offenbart, von denen er bei der Ausübung seines Berufes (oder bei der Ausbildung), der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag bestraft

58 David Rosenthal, Sanktionierung von Datenschutzverstössen, in: Nicolas Passadelis, David Rosenthal, Hanspeter Thür (Hrsg.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Helbling Lichtenhahn, Basel 2015, Rz. 7.89.

59 BGE 142 IV 315.

(Art. 56 E-DSG). Wie beim Berufsgeheimnis ist das Offenbaren geheimer Personendaten auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

[Rz 176] Die vorsätzliche Verletzung der beruflichen Schweigepflicht gemäss E-DSG – die fahrlässig begangene Tat ist nicht strafbar – wird mit einer Geldstrafe von bis zu CHF 250'000 bestraft und ist somit eine Übertretung. Dies im Gegensatz zu einem Verstoss gegen die Berufsgeheimnispflicht nach Art. 321 StGB, welche mit Haft bis 3 Jahren oder Geldstrafe bedroht wird und daher ein Vergehen darstellt.

[Rz 177] Für die im Spital tätigen Personen bringt diese Neuerung keine Änderungen, unterstehen sie doch bereits jetzt dem Berufsgeheimnis. Sei dies, weil sie einer zur Geheimhaltung verpflichteten Berufsgruppe angehören oder weil sie gemäss Art. 321 StGB als Hilfspersonen gelten.

2.4.19.4. Missachten von Verfügungen

[Rz 178] Ebenfalls mit Busse bis zu CHF 250'000 werden Personen bestraft, die einer vom EDÖB unter Hinweis auf die Strafdrohung von Art. 57 E-DSG ergangene Verfügung oder einem Entscheid der Rechtsmittelinstanzen vorsätzlich nicht Folge leisten (Art. 57 E-DSG).

2.5. Recht auf Datenportabilität wird nicht gewährt

[Rz 179] Das Recht auf Datenportabilität, das Recht also, dass die betroffene Person die über sie bearbeiteten Daten in einem Standardformat zurückerhalten und an einen anderen Anbieter übertragen kann, wird im E-DSG nicht geregelt. Dies im Gegensatz zur EU-DSGVO.

[Rz 180] Der Bundesrat vertritt die Auffassung, dass das Recht auf Datenportabilität mehr darauf ausgerichtet ist, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen. Daher gehöre eine solche Bestimmung nicht in das Datenschutzgesetz. Die Befürworter einer solchen Pflicht argumentieren, dass dadurch eine bessere Kontrolle über die Daten sichergestellt werde und somit sehr wohl ein Persönlichkeitsschutzaspekt vorliege.

[Rz 181] Somit besteht auch für Spitäler oder andere Leistungserbringer z.B. bei der Auskunftserteilung keine Pflicht, die Daten in einem Standardformat herauszugeben. Die Daten müssen ausschliesslich für den Patienten lesbar sein, was für alle Datenformate zutrifft, wenn man ein entsprechendes Programm mitliefert, um die Daten zu lesen.

3. Fazit

3.1. Bezüglich der EU-DSGVO

[Rz 182] Für diejenigen Spitäler, Praxen, Heime und Spitex, welche nicht aktiv den europäischen Markt bearbeiten, kommen die Bestimmungen der EU-DSGVO nicht zur Anwendung.

[Rz 183] Beim Betrieb einer Internetseite ist darauf zu achten, dass die Beobachtung des Verhaltens der europäischen Besucher der Internetseite nicht ein Tracking oder Profiling darstellt. Aufgrund der aktuellen Unsicherheit, welche Massnahmen als solches bezeichnet werden, sollte

man europäische Besucher im Sinne eines «dis-targetings» vom Tracking und Profiling ausnehmen.

Massnahme: Mit Hilfe von Geolokalisierungstools europäische Besucher der eigenen Internetseite im Sinne eines «dis-targetings» vom Tracking und Profiling ausnehmen.

3.2. Bezüglich des revidierten Datenschutzgesetzes

[Rz 184] Folgende Neuerungen des E-DSG führen bei Spitälern oder anderen Leistungserbringern zu Anpassungen. Dies auch dann, wenn sie bereits heute dem Datenschutz die nötige Beachtung schenken:

- Die Strafbestimmungen zielen auf Mitglieder des oberen Kaders der Spitäler, Praxen, Heime oder der Spitex. Sie müssen Organ eines Spitals sein oder als Mitarbeiter selbständige Entscheidungsbefugnisse im betroffenen Tätigkeitsbereich haben. Auf Antrag wird mit Busse bis zu CHF 250'000 bestraft, wer vorsätzlich Daten unrechtmässig ins Ausland bekannt gibt, die Datenbearbeitung unerlaubterweise einem Auftragsbearbeiter übergibt oder die Mindestanforderungen an die Datensicherheit nicht einhält.

  Massnahme: Die von der Strafdrohung betroffenen Personen müssen bezüglich dieser Neuerung informiert werden.

- Eine gewichtige Neuerung ist in der Datenschutz-Folgenabschätzung zu sehen und der Kontrollfunktion des EDÖBs, wenn die Unternehmung keinen qualifizierten Datenschutzberater hat. Die Datenschutz-Folgenabschätzung ist ein Instrument, um Risiken zu erkennen und zu bewerten, welche für die betroffenen Personen durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Sie ist z.B. vorab bei jeder Einführung eines neuen Klinikinformations- oder Laborsystems durchzuführen. Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung ein hohes Risiko für die Persönlichkeit der Patienten zur Folge hätte, wenn der Verantwortliche keine Massnahmen träfe, so muss vorgängig die Stellungnahme des EDÖB eingeholt werden. Auf die Konsultation des EDÖB kann verzichtet werden, wenn ein qualifizierter betrieblicher Datenschutzberater aktiv in die Erarbeitung der Datenschutz-Folgenabschätzung involviert war. Spitäler, Praxen, Heime oder die Spitex können von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn sie sich für die fragliche Bearbeitung einer Zertifizierung nach Art. 12 E-DSG unterzogen haben.

  Massnahme: Erarbeiten, wie eine Datenschutz-Folgeabschätzung durchgeführt wird.

- Die neue Bestimmung zum «Datenschutz durch Technik» führt dazu, dass die Spitäler und andere Leistungserbringer verpflichtet werden, Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die datenschutzkonforme Bearbeitung im System bereits so verwirklicht wird, dass die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausgeschlossen wird. Dies setzt voraus, dass die Spitäler, Praxen, Heime oder die Spitex über genügend Fachwissen verfügen, um «Privacy by Design» umzusetzen. Da Spitäler oder andere Leistungserbringer eine Vielzahl von besonders schützenswerten Personendaten bearbeiten, sind auch die damit verbundenen Risiken grösser. Folglich müssen auch die technischen Vorkehren hoch sein.

  Massnahmen: Prozesse für die Initialisierung von IT-Projekten überarbeiten und Datenschutzberater von Beginn an einbeziehen.

- Neu statuiert das E-DSG ein Melderecht bezüglich Daten Verstorbener an ihre Hinterbliebenen. Nach dem Tod darf – muss aber nicht – den Hinterbliebenen Einsicht in die Behandlungsakten gegeben werden. Wird dies verweigert, können die Hinterbliebenen die Aufsichtsbehörde des Spitals oder eines anderen Leistungserbringers kontaktieren und die Entbindung von der Berufsgeheimnispflicht verlangen.

  Massnahme: Prozess zur Herausgabe von Behandlungsunterlagen an Hinterbliebene anpassen.

- Der betriebliche Datenschutzverantwortliche erhält einen neuen Namen: Datenschutzberater oder Datenschutzberaterin. Spitäler, Praxen, Heime oder die Spitex welche einen solchen Berater in ihrem Betrieb installieren, haben gewisse Privilegien. So muss der EDÖB nach einer Datenschutz-Folgenabschätzung nicht konsultiert werden. Der Datenschutzberater muss qualifiziert und unabhängig sein. So darf er keine weiteren Aufgaben erfüllen, welche mit seinen Aufgaben als Datenschutzbeauftragter unvereinbar sind, so zum Beispiel, weil er zu einer Dienststelle gehört, die selbst besonders schützenswerte Personendaten bearbeitet.

  Massnahme: Prüfen, ob ein qualifizierter Datenschutzbeauftragter eingesetzt werden soll, damit man von den Privilegien profitieren kann.

- Verletzungen der Datensicherheit müssen dem EDÖB gemeldet werden, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit der betroffenen Person führt. Die Patienten selber müssen nur informiert werden, wenn dies der Schutz der betroffenen Person erfordert. Dies ist insbesondere der Fall, wenn die betroffene Person entsprechende Vorkehren zu ihrem Schutz treffen muss, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändert.

  Massnahmen: Prozess erarbeiten, wie im Bedarfsfall der EDÖB informiert wird. Prozess erarbeiten, wie im Bedarfsfall betroffene Patienten informiert werden könnten.

- Der Begriff der Datensammlung wird aufgehoben und es wird nur noch von «Bearbeiten» gesprochen. Folglich muss die Liste der Datensammlung umbenannt werden in «Verzeichnis der Datenbearbeitungstätigkeit».

  Massnahme: Liste der Datensammlungen in «Verzeichnis der Datenbearbeitungstätigkeit» umbenennen.

[Rz 185] Neuerungen, welche bei Spitälern und anderen Leistungserbringer, die bereits heute dem Datenschutz die nötige Aufmerksamkeit schenken, zu keinen Massnahmen führen:

- Die Regelung betreffend die Rechte der betroffenen Personen bringen für in der Medizin tätige Organisationen keine Neuerung. Aufgrund des engen Kontakts mit den Patienten und des durch das Vertrauen geprägten Miteinanders liegt immer eine Einwilligung des Patienten zur Datenbearbeitung vor.
- Die Informationspflicht wird umfassender ausgestaltet. Die Informationspflichten in der medizinischen Betreuung sind jedoch bereits heute durch die kantonalen Gesundheitsgesetze sehr stark ausgebildet. Darum bringt das E-DSG nichts Neues.
- Die Änderungen des grenzüberschreitenden Datenverkehrs treffen die Spitäler marginal, da dieser Verkehr in erster Linie von Art. 321 StGB bestimmt ist und nicht vom DSG oder neu vom E-DSG.

- Die neuen Bestimmungen zur Auskunftserteilung ändern nichts an der aktuellen Rechtslage der Spitäler und anderer Leistungserbringer. Weiterhin sind sie verpflichtet, dem Patienten gratis Kopien seiner Behandlungsunterlagen zuzustellen.
- Neu werden nur noch die Personendaten von natürlichen Personen (Patienten, freipraktizierende Ärzte oder Pflegefachleute) durch das DSG geschützt. Die Daten von juristischen Personen, also z.B. eines Spitals, eines Heims oder einer als AG organisierten Praxisgemeinschaft, nicht.
- Der Begriff «Inhaber der Datensammlung» gibt es im E-DSG nicht mehr. Er wird durch den Begriff «Verantwortlicher» ersetzt. Gemeint ist weiterhin das Gleiche: die Organisation, welche die Daten bearbeitet.
- Des Weiteren wird die berufliche Schweigepflicht von Art. 321 StGB ausgeweitet, was jedoch für Angestellte eines Spitals oder anderer Leistungserbringer keine Auswirkung hat, da diese bereits heute der beruflichen Schweigepflicht unterstehen (ungeachtet der Funktion).

Dr. iur. Christian Peter, CAS Information Security and Risk Management ist Partner der HEP & Partner GmbH und unterstützt Organisationen im Gesundheitswesen u.a. in datenschutzrechtlichen Belangen.