# Darauf muss jetzt geachtet werden

Die **Datenschutz-Grundverordnung der Europäischen Union** (DS-GVO) trat am 25. Mai 2018 in Kraft, gleichzeitig laufen die Revisionen des nationalen und der kantonalen Datenschutzgesetze. Was hat sich für Heime und Spitäler geändert und was ist zu erwarten?

▶ CHRISTIAN PETER

Die europäische Datenschutz-Grundverordnung (DS-GVO) hat zum Ziel, den Schutz von Personen in der Europäischen Union (EU) auch gegenüber Dienstleistern sicherzustellen, die ihren Sitz ausserhalb der EU haben. Die Bürger sollen den Schutz nicht verlieren, nur weil ein Dienstleister nicht in der EU angesiedelt ist, die Dienstleistungen aber trotzdem in der EU anpreist (Marktortprinzip).

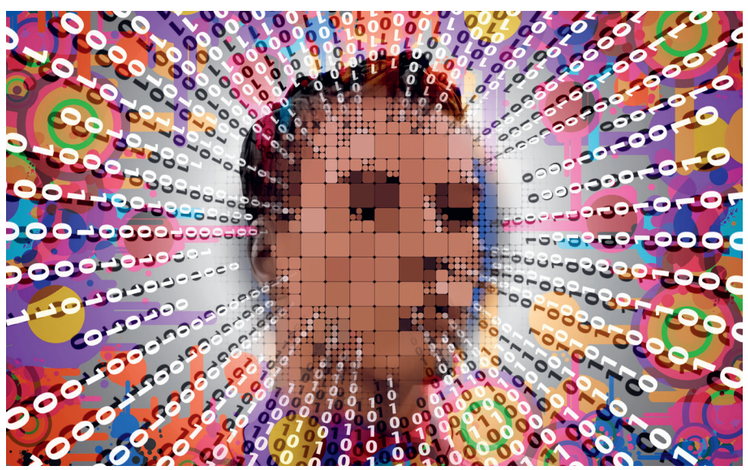
Somit ist für Schweizer Spitäler und Heime entscheidend, ob sie ihre Dienstleistungen auch in den Ländern der EU anbieten. Die meisten Schweizer Spitäler und Heime richten ihre Dienstleistungen nicht aktiv an Personen in der EU aus – beispielsweise durch eine gezielte Ansprache von Personen in anderen Ländern über ihre Webseite – und erbringen ihre Dienstleistung auch nicht in der EU. Somit müssen sie sich auch nicht dem europäischen Recht unterwerfen. Es sei denn, sie beobachten Personen in der EU über ihre Website. Dies kann der Fall sein, wenn sie das Surfverhalten von identifizierbaren Personen in der EU verfolgen. Mit einer Umprogrammierung der Seite kann das jedoch verhindert werden.

Eine Anwendbarkeit der DS-GVO ist ebenfalls nicht gegeben, wenn sich ein EU-Kunde ausschliesslich auf eigene Initiative für die Dienstleistung entscheidet, beispielsweise ein Tourist, der sich behandeln lässt. Auch führt die Beschäftigung oder die Rekrutierung von EU-Bürgern nicht zu einer Anwendbarkeit.

## Nationale Datenschutzrevision kommt

Ungeachtet der Anwendbarkeit der DS-GVO gilt jedoch zu beachten, dass sich auch die bevorstehenden Schweizer Revisionen an der europäischen Norm orientieren werden. Die Schweiz möchte, dass die EU weiterhin anerkennt, dass die Eidgenossenschaft über ein angemessenes Datenschutzniveau verfügt. Wann die revidierten Erlasse in Kraft treten werden, ist noch offen. Die Revision des nationalen Rechts wurde in zwei Teile aufgeteilt und das für die Spitäler und Heime relevante zweite Paket wird erst in der Wintersession 2018 vom Nationalrat als Erstrat behandelt, sodass das revidierte Gesetz frühestens in der zweiten Hälfte 2019 in Kraft treten wird. Bei den Kantonen ist es sehr unterschiedlich, während der Kanton Aargau sein neues Recht auf den 1. August 2018 in Kraft treten lassen will, wurde im Kanton Bern noch nicht einmal eine Vernehmlassung gestartet. Auf jeden Fall werden die Revisionen alle dieselbe Stossrichtung haben – die der DS-GVO. In Zukunft wird verlangt, dass die Betriebe nachweisen können, dass sie die Datenschutzbestimmungen einhalten. Es reicht somit nicht mehr aus, den Datenschutz im Einzelfall zu beachten, sondern der Betrieb muss nachweisen können, dass dies systematisch geschieht. Dieser Nachweis kann z. B. mittels Etablierung eines sogenannten Datenschutzmanagementsystems (DSMS) erbracht werden.

Nur wenn die Betroffenen wissen, was mit ihren Daten geschieht, können sie auch entscheiden, ob sie das wollen. Durch Transparenz soll den Betroffenen die Entscheidungsgewalt über ihre Daten wieder zurückgegeben werden. Spitäler und Heime müssen ihren Patienten und Kunden daher genau erklären, welche Daten erhoben werden, was mit ihnen gemacht wird und ob sie Dritten (z.B. Kostenträgern) weitergegeben werden.



Die neue Pflicht, ein Verzeichnis der Bearbeitungstätigkeiten zu erstellen, wird die Meldepflicht der Datensammlungen nach bisherigem Recht ersetzen. Das Verzeichnis soll Auskunft darüber erteilen, welche Daten das Spital oder Heim auf welche Weise bearbeiten. Also muss beispielsweise der Bearbeitungszweck, die Kategorie der Personendaten, der Empfänger der Daten und die Aufbewahrungsdauer vermerkt werden. Dieses Verzeichnis ist kein bürokratischer Leerlauf, sondern ist auch für die Betriebe von grösstem Interesse. Denn es hält fest, welche Daten im Betrieb in welchen Systemen anfallen und welchen Gefahren sie ausgesetzt sind. So sind die Betriebe erst in der Lage, sich über die gesetzlich geforderten Sicherheitsvorkehrungen Gedanken zu machen.

## Meldung von Datenschutzverletzungen

In Zukunft müssen Verletzungen der Datensicherheit gemeldet werden. Das betrifft nicht kleinere, unbedeutende Verletzungen, wie beispielsweise ein einzelner Fehlzugriff in einem Informationssystem. Nur wenn eine Verletzung dazu führt, dass Personendaten verloren, verändert oder zugänglich gemacht werden und hieraus ein hohes Risiko für die Persönlichkeit der betroffenen Personen entsteht, muss eine Meldung erfolgen. In der Regel reicht eine Information an den behördlichen Datenschutzbeauftragten aus. Nur wenn es zum Schutz der betroffenen Personen erforderlich ist, müssen diese direkt informiert werden. Zum Beispiel dann, wenn sie ihre Zugangsdaten oder Passwörter ändern müssen.

Mit der Pflicht zur Datenschutz-Folgenabschätzung sollen Risiken, die beim Einsatz von Datenbearbeitungsvorhaben entstehen können, erkannt und bewertet werden. Auf der Basis dieser Abschätzung können anschliessend angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu minimieren. Ziel ist es, allfällige datenschutzrechtliche Probleme präventiv anzugehen und dadurch nicht zuletzt Kosten zu sparen. Da bei Heimen und Spitälern sehr oft sehr umfangreich besonders schützenswerte Daten bearbeitet werden, ist davon auszugehen, dass bei allen Informationssystemen eine Datenschutz-Folgeabschätzung durchzuführen ist und anschliessend definiert werden muss, mit welchen Massnahmen diese Risiken bewältigt werden sollen.

Ein weiteres zentrales Element der Revisionen der Datenschutzgesetze ist die Stärkung der Betroffenenrechte. Personen sollen besser als früher über ihre Daten bestimmen können und es soll ihnen leichter fallen, die Nutzung ihrer Daten zu kontrollieren. Hierzu brauchen sie zum einen Informationen und zum anderen die Möglichkeit ihre Anliegen anzubringen. Ein klarer Ansprechpartner ist hierfür unabdingbar. An diesen können sie dann beispielsweise ihr Auskunftsbegehren stellen. Nur wenn sie Informationen über die Datenbearbeitung haben, können sie anschliessend beantragen, dass die Daten berichtigt, gesperrt oder gelöscht werden. Wobei der Löschung von Behandlungsdaten die Pflicht der Behandelnden, die Behandlung zu dokumentieren, entgegensteht und somit eine Löschung von Behandlungsdaten während der Aufbewahrungspflichten nicht möglich ist.

## Bussen keine Bedrohung

Auch wenn vor allem im Zusammenhang mit dem europäischen Recht die Bussen immer wieder als riesiges Damoklesschwert bezeichnet wurde, ist diese Bedrohung zu relativieren. Zwar sieht das nationale Recht auch Bussen vor (die kantonalen Gesetze verzichten regelmässig auf Bussen), und zwar für Leitungspersonen, welche weitreichenden Entscheidungsbefugnisse haben, doch diese gibt es bereits im aktuellen Recht und nur vorsätzliches Handeln wird bestraft und dies auch nur, wenn Informations-, Melde- und Auskunftspflichten verletzt werden. Begeht man somit fahrlässig eine Datenschutzverletzung, drohen weder Busse noch Haft.

Zusammenfassend ist festzuhalten, dass die neuen Datenschutzbestimmungen bei Heimen und Spitälern nicht zu Aktivismus führen muss. Vielmehr ist angezeigt, die Änderungen im nationalen und kantonalen Recht zu beobachten und mit Augenmass umzusetzen. Der Datenschutz ist schon längst zu einer selbstverständlichen Leistung in einer serviceorientierten Dienstleistungsgesellschaft geworden und wo dem Datenschutz nicht die notwendige Aufmerksamkeit gewidmet wird, da ist die Ausrichtung letztlich auch nicht patientenbezogen.

### H+ Bildung

Christian Peter referierte zu diesem Thema im Rahmen der H+Bildung-Tagung «Datenschutz und elektronisches Patientendossier im Spitalalltag» am 13. Juni 2018 in Zürich. Aufgrund der grossen Resonanz plant H+ Bildung eine weitere Veranstaltung in Bern im Dezember.

H+ Bildung bietet laufend für nahezu alle Berufsgruppen und Funktionen in Spital, Pflegeinstitution sowie Spitex hochwertige Weiterbildungen an – auch speziell konzipiert oder betriebsintern durchgeführt.

› **www.hplus-bildung.ch**

**Dr. iur. Christian Peter** ist Partner bei HEP & Partner und arbeitet seit über 14 Jahren als Jurist für Spitäler, Heime und Verbände im Gesundheitswesen; sei dies als Rechtskonsulent oder als externer betrieblicher Datenschutzbeauftragter.