DSGVO, Cyber & Co.: Was müssen Ärztinnen und Ärzte beachten?*

Liliane Mollet

Juristin und Datenschutzverantwortliche der FMH

Ärztinnen und Ärzte erfahren tagtäglich äusserst sensible und intime Informationen über ihre Patientinnen und Patienten. Daher ist ihre Verantwortung bezüglich Datenschutz und Datensicherheit entsprechend hoch. Diese Daten gehören zur Kategorie der «besonders schützenswerten Personendaten» und werden durch das schweizerische Datenschutzgesetz entsprechend stark geschützt. Zusätzliche Anforderungen können sich aus der am 25. Mai 2018 wirksam gewordenen europäischen Datenschutz-Grundverordnung (DSGVO) ergeben. Die wichtigsten Punkte.

DSGVO: Worum geht es?

Mit der neuen Verordnung DSGVO hat die EU ein umfassendes Regelwerk zum Schutz personenbezogener Daten ins Leben gerufen. Wichtigste Auslöser hierfür waren einerseits die rasante Vernetzung und kontinuierliche Digitalisierung aller Lebensbereiche und andererseits die unterschiedlichen Datenschutzniveaus der einzelnen EU-Staaten, welche den fairen Wettbewerb beeinträchtigten. Personendaten werden heute rege gesammelt, miteinander verknüpft und zu neuen Informationen verarbeitet. Für natürliche Personen wie Ärztinnen und Ärzte sowie Patientinnen und Patienten wird es immer schwieriger zu erkennen, welche Daten wo gespeichert sind, wer darauf Zugriff hat und wie diese tatsächlich bearbeitet werden. Dies führt dazu, dass sie in ihrer informationellen Selbstbestimmung, also der Freiheit zu entscheiden, ob und wie ihre Daten genutzt werden, eingeschränkt werden. Auch ihre gesetzlichen Rechte können sie damit nicht mehr richtig wahrnehmen (z.B. das Recht auf Auskunft oder die Mitbestimmung bei von Software-Programmen gefällten Entscheiden). Dies, weil ihnen die notwendige Transparenz im Umgang mit ihren Personendaten fehlt. Sie alle sollen wieder eine bessere Kontrolle über ihre eigenen Personendaten erhalten. Deshalb erfährt die Datenschutzgesetzgebung europaweit (inkl. der Schweiz) eine umfangreiche Revision. So sind auch die «Schengen-Richtlinie» und die «Europaratskonvention 108» revidiert worden. Diese beiden internationalen Abkommen sind für die Schweiz verbindlich. Daher ist die Schweiz verpflichtet, ihr eigenes Datenschutzgesetz entsprechend anzupassen. Da sich die Abkommen inhaltlich stark an der DSGVO ausrichten und Schweizer Unternehmen aufgrund unterschiedlicher Regelungen wirtschaftlich nicht benachteiligt werden sollen, wird sich das künftige schweizerische Datenschutzgesetz inhaltlich an der DSGVO orientieren. Schweizer Unternehmen, welche bereits heute die DSGVO umsetzen, werden auch für das neue DSG bereit sein.

Europäisches Recht für Schweizer Arztpraxen und Spitäler?

Die DSGVO gilt grundsätzlich nur für die EU (seit dem 20. Juli 2018 auch für die EWR-Mitglieder). Im Kontext der EU bzw. der DSGVO wird die Schweiz, da Nicht-EU- bzw. -EWR-Mitglied, als Drittstaat betrachtet. Heisst, dass für Schweizer Unternehmen weiterhin das schweizerische Datenschutzgesetz gilt. Jedoch sieht die DSGVO Fälle vor, wo die Berührung mit der EU als so stark angesehen wird, dass sich die Anwendung der DSGVO auch für Drittstaaten rechtfertigt. Sollte eine Arztpraxis oder ein Spital seine Dienstleistungen klar auch an Patientinnen und Patienten richten, welche sich in der EU befinden, dann ist die DSGVO anwendbar. Dasselbe gilt, wenn die betreffende Arztpraxis oder das Spital eine Zweigniederlassung in der EU hat. Weiter ist die DSGVO anwendbar, wenn z.B. über die Website der Arztpraxis oder des Spitals das Verhalten von Website-Besucher «beobachtet» wird, welche sich in der EU befinden. Dies kann z.B. mittels Einsatz von Cookies oder Webanalyse-Tools wie Google Analytics

* Dieser Artikel ist bereits in der *Synapse* erschienen (Mollet L. DSGVO, Cyber & Co.: Was müssen Ärztinnen und Ärzte beachten? Synapse. 2018;4:5–7).

der Fall sein. Abschliessend kann dies jedoch nur unter Betrachtung der konkreten Situation der jeweiligen Arztpraxis bzw. des jeweiligen Spitals beurteilt werden.

Was ändert sich mit der neuen Datenschutzgesetzgebung?

Die DSGVO ist nicht etwas völlig Neues. Viele darin enthaltene Grundsätze und Rechte sind bereits im schweizerischen Datenschutzgesetz enthalten (so z.B. der Grundsatz der «Datenminimierung» bzw. der «Verhältnismässigkeit»). Bereits vor der DSGVO galten gesetzlich festgelegte Grundsätze, wie Daten für welche Zwecke erhoben und verarbeitet werden dürfen. Doch verschärft die DSGVO gewisse Regelungen und verpflichtet den Verantwortlichen (natürliche Person oder Organisation, die Personendaten bearbeitet) auch zu transparenterer und nachvollziehbarer Dokumentation der erhobenen Daten. Ausserdem sieht die DSGVO empfindliche Sanktionen bei Verletzung der neuen Datenschutzbestimmungen vor. Dies gilt auch für den Alltag der Ärztinnen und Ärzte in der Schweiz: Grundsätzlich ändert sich bezüglich der Bearbeitung von Personendaten nicht viel. Allerdings müssen sie künftig noch konkreter informieren, mehr dokumentieren und nachweisen. Heisst, dass alle natürlichen Personen, über welche Daten bearbeitet werden, entsprechend darüber Bescheid wissen (insbesondere mittels eines Vertrages, Information auf dem Patientenanmeldeformular und/oder einer Datenschutzerklärung auf der Website).

Welche Aspekte müssen Ärztinnen und Ärzte beachten?

Ungeachtet der Anwendbarkeit der DSGVO empfiehlt es sich, gewisse Punkte im Hinblick auf die Bearbeitung von Patientendaten zu evaluieren und zu dokumentieren. Die Anforderungen und Grundsätze der DSGVO können hierbei als Grundlage dienen.

1. Situationsanalyse

Ausgangslage sollte immer die Gesamtsicht («Big Picture») aller Daten, Systeme und Zusammenhänge sein. Mit Hilfe einfacher, genereller Fragen und Antworten kann rasch eine erste Übersicht über die Situation der Arztpraxis oder des Spitals geschaffen werden: Ist die DSGVO überhaupt anwendbar? Standort/e der Arztpraxis oder des Spitals? An wen richten sich die Dienstleistungen? Anzahl internes und externes Personal? Durchschnittliche Anzahl Patientinnen und Patienten? Anzahl Arbeitsplätze, Applikationen und Server mit Anschluss ans Internet? Wo befinden sich die Patientendaten (in der Arztpraxis bzw. dem Spital oder in einer Cloud oder auf Papier)? Dies sind bereits einige Punkte, welche eine grobe Sicht der Situation vermitteln. Sie bilden ausserdem eine wichtige Grundlage für die individuelle Risikobeurteilung.

2. Risikobasiertes Vorgehen: Prioritäten setzen

Je nach Einschätzung der persönlichen Situation (z.B. zentraler oder ländlicher Standort; regelmässige Datentransfers in unsichere Drittstaaten; umfangreiche digitale Prozesse mit heiklen Patientendaten oder wenige überschaubare Applikationen; u.a.) sowie der Risikobereitschaft («Risiko-Appetit») sind höhere oder gemässigtere Datenschutzmassnahmen notwendig. Bei einem hohen Risiko für die betroffenen Patientinnen und Patienten ist für einen bestimmten Prozess oder eine Applikation womöglich auch eine Datenschutz-Folgenabschätzung (eine Art Risikoanalyse in Bezug auf die konkrete Datenbearbeitung und deren mögliche Auswirkungen auf die betroffenen Personen) notwendig. Prioritäten sollten auf kritische Themen wie insbesondere Patientendaten und -rechte sowie Personaldaten gesetzt werden. Auch der eigene Webauftritt bzw. die Sichtbarkeit gegen aussen steht im besonderen Fokus, weil dieser meist die erste Anlaufstelle für Patientinnen und Patienten wie auch für Datenschutzaufsichtsbehörden darstellt. Zudem bietet gerade die eigene Website grosses Potential, um die erforderliche Datenschutz-Compliance nachzuweisen und Kompetenz zu zeigen. So kann über die Website bereits ein wichtiger Beitrag zur Informationspflicht geleistet und auf Betroffenenrechte (z.B. das Auskunftsrecht) hingewiesen werden. Sie ersetzt jedoch nicht die konkrete Information der Patientinnen und Patienten (siehe nachstehend).

3. Verzeichnis aller kritischen Datenbearbeitungen («Data Mapping»)

Eine Bestandsaufnahme aller kritischen Datenbearbeitungen, die in der Zuständigkeit der Arztpraxis oder des Spitals liegen, sollte vorgenommen werden. Hierbei ist es unbeachtlich, in welcher Form die Personendaten vorliegen (elektronische Daten, Papierform oder Röntgenbilder u.a.). Das Verzeichnis muss die gesetzlich vorgeschriebenen Mindestangaben enthalten (z.B. Namen und Kontaktdaten des Verantwortlichen, die Art der Daten, Bearbeitungszweck und Datenempfänger). Weitere sinnvolle Angaben sind die Rechtsgrundlage, worauf die jeweilige Datenbearbeitung beruht (z.B. Einwilligung des Patienten, Erfüllung eines Vertrages, berechtigtes Interesse der Ärztin oder des Arz-

tes u.a.), sowie die getroffenen organisatorischen und technischen Massnahmen zum Schutz der Personendaten. Dieses Verzeichnis gilt zugleich als Nachweis der Compliance (Dokumentationspflicht / Grundsatz der Accountability). Verschiedene Muster und Vorlagen für Datenverzeichnisse finden sich im Internet (siehe unter «Weiterführende Links» am Ende dieses Artikels).

4. Interne Datenschutzrichtlinie(n)

Hierbei handelt es sich um ein Regelwerk zur Bearbeitung von Personendaten. Die Datenschutzrichtlinie enthält verbindliche und zentrale Vorgaben zum Umgang mit Personendaten in der Arztpraxis oder im Spital. Ähnlich wie eine «Hausordnung» sind alle Mitarbeitenden der Arztpraxis bzw. des Spitals zur Einhaltung dieser Richtlinien verpflichtet. Sie dienen der Klarheit und legen die Grundlage für ein gemeinsames Verständnis und einheitlichen Umgang mit Personendaten fest. Die Richtlinie sollte mindestens die schweizerischen Datenschutzgrundsätze enthalten (siehe dazu die Übersicht der Datenschutzgrundsätze, im Anhang zu den Richtlinien von 2014 über die Mindestanforderungen an das DSMS, welche im Rahmen von Datenschutzzertifizierungen verwendet wird). Weitere wichtige Inhalte sind z.B. klar zugewiesene Verantwortlichkeiten, Regeln im Umgang mit Patientendaten und das Vorgehen bei Ausübung der Betroffenenrechte (z.B. Auskunftsrecht u.a.).

5. Personal; Arbeitsverhältnisse/-verträge

Alle Mitarbeitenden der Arztpraxis oder des Spitals sollten grundsätzlich schriftlich zur Geheimhaltung sowie Einhaltung der definierten Datenschutzrichtlinien verpflichtet werden. Diese Verpflichtung in Kombination mit einer regelmässigen Sensibilisierung und Schulung hinsichtlich Datenschutz und Sicherheit trägt wesentlich zum Schutz der Personendaten bei.

Sind EU-Bürgerinnen und EU-Bürger z.B. als Grenzgänger in der Arztpraxis tätig, dann könnte sich die Frage stellen, ob allenfalls die DSGVO auf diese Arbeitsverhältnisse anwendbar ist. Dies ist grundsätzlich zu verneinen, da die DSGVO sich auf das Angebot von Waren oder Dienstleistungen von der Schweiz in die EU bezieht. Der Arbeitgeber bietet jedoch weder Waren noch Dienstleistungen i.S.v. Art. 3 Abs. 2 lit. a DSGVO in die EU an. Zudem befinden sich die EU-Bürgerinnen und EU-Bürger im Zeitpunkt der Erbringung ihrer Arbeitsleistung und der damit verbundenen Datenbearbeitung in der Schweiz. Daher fallen die Nachfrage von Arbeitsleistung in der EU sowie die Arbeitsverhältnisse in der Schweiz nicht unter die DSGVO.

6. Patientinnen und Patienten; Betroffenenrechte

Personendaten wie Patientendaten dürfen nur bearbeitet werden, wenn hierfür eine entsprechende Rechtsgrundlage besteht. Patientendaten sind per Gesetz besonders schützenswert und daher, wie bereits erwähnt, mit entsprechend hoher Sorgfalt zu behandeln. Ausserdem können auch Patientinnen und Patienten gegenüber ihrem Arzt jederzeit die gesetzlich verankerten Datenschutzrechte wahrnehmen.

a) Einwilligung

Grundlage der Behandlung von Patientinnen und Patienten bildet der Behandlungsvertrag zwischen Arzt und Patient. Die Bedingungen dieses Vertrages ergeben sich in erster Linie aus dem kantonalen Spital- oder Gesundheitsrecht. Zur Bearbeitung von Patientendaten, weil besonders schützenswert, benötigt es ausserdem eine ausdrückliche Einwilligung des Patienten. Der Arzt oder das Spital muss nachweisen können, dass die betroffene Person in die Bearbeitung ihrer Daten zum erwähnten Zweck eindeutig (= durch eine aktive Handlung) und freiwillig (= ohne Zwang) eingewilligt hat. Dies gilt auch wenn Personendaten an Dritte (z.B. Ärztekassen oder Inkasso-Unternehmen) weitergegeben oder für andere Zwecke (z.B. medizinische Forschung) bearbeitet werden sollen. Zudem muss das Ersuchen um Einwilligung «in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache» erfolgen. Ausserdem muss diese Einwilligung klar von anderen Sachverhalten getrennt sein. Wichtig ist zudem der Hinweis darauf, dass die Einwilligung jederzeit widerrufen werden kann (Widerrufsrecht).

b) Informationspflicht

Mit der DSGVO werden höhere Anforderungen an die Informationspflicht gestellt. Ärztinnen und Ärzte müssen ihre Patienten aktiv hinsichtlich der Erhebung und Speicherung von Personendaten informieren. Diese Information muss in «präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache» erfolgen. Insbesondere müssen folgende Punkte mitgeteilt werden: Ansprechpartner und Kontaktdaten; Zwecke, für welche die Personendaten bearbeitet werden; die entsprechende Rechtsgrundlage und gegebenenfalls die Datenempfänger. Sollten die Personendaten nicht bei der betroffenen Person (Patienten) erhoben worden sein, dann ist ausserdem die Art der Daten mitzuteilen. Die Informationspflicht kann beispielsweise mittels einer Information über die Website der Arztpraxis oder des Spitals, Plakate im Wartsaal oder auf dem Formular der Patientenanmeldung wahrgenommen werden.

c) Recht auf Auskunft
Dieses Recht existiert seit langem auch im schweizerischen Datenschutzgesetz. Hierbei hat jede Patientin/jeder Patient das Recht zu erfahren, welche Daten über sie gespeichert sind bzw. aufbewahrt werden. Gestützt auf diese Auskunft kann die betroffene Person ihre Datenschutzrechte wie das Recht auf Datenportabilität oder Recht auf Löschung wahrnehmen und damit die Kontrolle über die eigenen Daten behalten. Hierfür muss die betroffene Person selber aktiv werden und dieses Recht gegenüber der Ärztin oder dem Arzt wahrnehmen.

d) Recht auf Löschung
Personendaten wie auch Patientendaten dürfen nicht unbeschränkt aufbewahrt und/oder archiviert werden (Stichwort «Recht auf Vergessen»). Hierfür gibt es gesetzliche Aufbewahrungs- und Löschungsfristen zu beachten. Die vorgängig erwähnte Datenschutzrichtlinie ist ein gutes Instrument, um solche Fristen und Prozesse festzuhalten. Ärztinnen und Ärzte sollten sich ausserdem bewusst sein, dass nicht in jedem Fall das Recht auf Löschung gilt, sondern gewisse gesetzliche Aufbewahrungsfristen gelten.

7. Externe Dienstleister und Dritte
Verträge mit externen Dienstleistern (z.B. Informatikdienstleister oder Ärztekassen) sollten grundsätzlich einmal auf ihre Vereinbarkeit mit den neuen datenschutzrechtlichen Vorschriften (DSGVO) sowie im Hinblick auf die anstehende Datenschutzgesetzrevision in der Schweiz überprüft und wo nötig angepasst werden. Sobald Patientendaten elektronisch und in Applikationen wie Praxissoftware verarbeitet werden, sind meistens Auftragsverarbeiter wie Informatikdienstleister zur Betreuung dieser Systeme involviert. Hierbei kann es sein, dass externe ICT-Mitarbeitende auf die Praxissoftware zugreifen und allenfalls auch Einsicht in Patientendaten erhalten. Die DSGVO legt die Anforderungen genau fest, welche mit Auftragsverarbeitern neu zum Schutz von Personendaten geregelt werden müssen (z.B. als Anhang zum bereits bestehenden Support- oder Wartungsvertrag). Insbesondere sind der Auftragsverarbeiter und seine Mitarbeitenden schriftlich zur Geheimhaltung zu verpflichten. Grössere Informatikdienstleister werden inzwischen bereits entsprechende Vereinbarungen/Vertragszusätze unter Berücksichtigung der DSGVO zur Unterzeichnung unterbreitet haben.

8. Daten- und Cybersicherheit
Cyberkriminalität wie das Hacken von Spitalnetzen oder der Verkauf von Patientendaten im sogenannten «Darknet» ist in aller Munde. Das Risiko, dass Patientendaten für kriminelle Zwecke wie Identitätsdiebstahl oder Phishing missbraucht werden könnten, nimmt stetig zu. Die steigende Digitalisierung verschärft die Situation zusätzlich. Eine hundertprozentige Sicherheit wird es nie geben. Aufgeben? Nein! Sondern den Fokus auf den Basisschutz von Computern und mobilen Geräten legen, regelmässig überprüfen und optimieren (einmal mehr: risikobasierter Ansatz). So ist z.B. der Mensch wie das interne oder externe Personal weiterhin das grösste Sicherheitsrisiko und nicht die Technik! Daher ist eine mehrschichtige Sicherheit anzustreben. Heisst, dass organisatorische Massnahmen (insbesondere regelmässige Sensibilisierungen und Schulungen) entsprechend kombiniert mit technischen Massnahmen (z.B. aktuelle Personal-Firewalls auf allen Geräten, periodische Updates aller Programme usw.) den effektivsten Schutz darstellen. Auch hierfür finden sich grundsätzliche Hilfestellungen im Internet (siehe unter «Weiterführende Links»). Diese Massnahmen sollten mit der individuellen Risikobeurteilung abgestimmt sein. Schliesslich müssen die durch die Arztpraxis oder das Spital getroffenen Massnahmen ebenfalls entsprechend dokumentiert sein und nachgewiesen werden können.

Weiterführende Links

- EDÖB – Erläuterungen zum Datenschutz in der Arztpraxis: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/erlaeuterungen-zum-datenschutz-in-der-arztpraxis.html
- BSI für Bürger – nützliche Empfehlungen und Checklisten für die Sicherheit in der Arztpraxis und zu Hause, wie z.B.: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html
- DSAT – Datenschutz Self Assessment Tool für Schweizer Unternehmen mit Vorlagen und Mustern zur Umsetzung der DSGVO: http://dsat.ch/
- Kassenärztliche Bundesvereinigung – Beispiele, Muster und Vorlagen zur Umsetzung der DSGVO: http://www.kbv.de/html/1150_34037.php

Korrespondenz:
FMH
Datenschutzverantwortliche
Elfenstrasse 18
Postfach 300
CH-3000 Bern 15
datenschutz[at]fmh.ch