Inhalt

1. Einleitung und Allgemeines

1.1. Neuregelung des Datenschutzes in Deutschland 2016

1.1.1. Die Einführung der DSGVO

Schon 1995 gab es eine Europäische Richtlinie zum Datenschutz, die 2001 in Form des Datenschutzgesetzes in nationales Recht umgewandelt wurde. Seitdem gab es fast zwanzig Jahre lang keine Änderung mehr im Deutschen Datenschutz.

Seit dem 25.05.2018 ist die Europäische Datenschutzgrundverordnung (EU-DSGVO) der Europäischen Union in vollem Maße in Deutschland in Kraft getreten. Als Europäische Verordnung ist sie unmittelbar wirksam und muss nicht erst in nationales Recht umgewandelt werden. Es ist direkt in der DSGVO geregelt, wo die Mitgliedsstaaten keine Änderungen vornehmen dürfen und wo Abweichungen je nach Staat möglich sind (das sind dann so genannte „Öffnungsklauseln“).

Die DSGVO ist immer noch für alle neu, auch für die Behörden. Diese Tatsache, gepaart mit dem Föderalismus in Deutschland, sorgt nach wie vor für große Unsicherheit, was denn in welchen Fällen zu unternehmen ist und was bei Nichterfüllung droht. So werden Details der DSGVO je nach Bundesland unterschiedlich interpretiert.

1.1.2. Zum Fachtext

Gerade wegen dieser Unsicherheiten haben wir beschlossen, diesen Fachtext zu schreiben. Das Thema Datenschutz scheint recht weit vom Urinlabor entfernt, bei genauerer Betrachtung ist dies jedoch nicht so. Über die Arbeit im Labor kommen wir zum Arbeitsschutz, vom Arbeitsschutz kommt man unter anderem zum Datenschutz.

Der Fachtext soll die wichtigsten Grundprinzipien im Datenschutz widerspiegeln und die wichtigsten Forderungen aus der Verordnung zusammenfassen. Er soll auch so gut wie möglich darstellen, was in der Urologischen Praxis umzusetzen ist und was man sich eher sparen kann.

1.2. Rechtliche Grundlagen

1.2.1. Die Bedeutung der DSGVO

Die Verordnung betrifft die Verarbeitung von personenbezogenen Daten innerhalb der EU bzw. von EU-Bürgern. Dabei spielt es keine Rolle, ob die Erhebung der Daten automatisch oder durch Menschen erfolgt. Die DSGVO schützt nur personenbezogene Daten, Daten von Firmen und Unternehmen sind nicht betroffen. Es geht dabei um die geschäftsmäßige Nutzung von Daten, nicht um die private Nutzung.

1.2.2. Das neue BDSG

Das Bundesdatenschutzgesetz (BDSG) ist erneuert worden und am 25.05.2018 in Kraft getreten. Das BDSG ist als Ergänzung der DSGVO gedacht und regelt nationale Besonderheiten. In Einzelfällen gibt es Konfliktpunkte, die in Zukunft noch geklärt werden müssen. Das ist für die Arbeit in der Arztpraxis aber weitestgehend unerheblich.

1.2.3. Weitere Gesetze zum Datenschutz

Es gibt verschiedene Gesetze, welche auch stellenweise Aussagen zum Datenschutz treffen. Dazu gehört das Sozialgesetzbuch, das Telekommunikationsgesetz, das Betriebsverfassungsgesetz und das Infektionsschutzgesetz. Das IfSG regelt zum Beispiel Meldepflichten. Meldepflichten hebeln in einigen Fällen den Datenschutz aus.

1.3. Definitionen

1.3.1. Datenschutz und Datensicherheit

Datenschutz und Datensicherheit sind nicht dasselbe. Beim Datenschutz geht es darum, welche Daten von wem genutzt werden dürfen und zu welchem Zweck. Bei der Datensicherheit geht es darum, wie genutzte Daten gegen den Zugriff Dritter gesichert werden. Die Datensicherheit ist damit ein Bestandteil des Datenschutzes.

1.3.2 Die Akteure im Datenschutz

Die am Datenschutz Beteiligten sind die Verantwortlichen, die Betroffenen und die Dritten. Ein Verantwortlicher ist derjenige, der Daten erhebt und diese Daten verarbeitet. Ein Betroffener ist derjenige, dessen Daten gesammelt und verarbeitet werden. Ein Dritter ist jemand, der, aus welchen Gründen auch immer (berechtigt oder unberechtigt), Einsicht in die Daten des Betroffenen erhält, oder erhalten kann.

Der Datenschutzbeauftragte dient in einem Unternehmen als Ansprechpartner in Sachen Datenschutz, sowohl für das Unternehmen als auch für mögliche Betroffene und auch für die Behörden. Ein Datenschutzbeauftragter kann intern oder extern sein; er sollte schriftlich benannt werden. Der Begriff ist leider nicht geschützt, das heißt es ist nicht geregelt, welche Qualifikation der Datenschutzbeauftragte besitzen muss. Er muss nur über die notwendige „Fachkunde“ verfügen.

1.3.3. Personenbezogene Daten und sensible Daten

Persönliche Daten sind alle Angaben zu einer natürlichen Person (Größe, Hobbys, Geburtsdatum). Sensible Daten sind personenbezogene Daten von besonderer Bedeutung. Das sind zum Beispiel Daten, die zur Diskriminierung z.B. bei einer Bewerbung auf eine Arbeitsstelle oder ein Amt genutzt werden könnten, wie sexuelle Orientierung, Parteizugehörigkeiten, Religionszugehörigkeit. Auch medizinische Daten gelten normalerweise als sensible Daten.

2. Grundprinzipien des Datenschutzes

2.1. Rechtliche Grundlagen der Datennutzung

Für die Benutzung von persönlichen Daten gilt das Rechtsprinzip „Verbot mit Erlaubnisvorbehalt“. Das bedeutet nichts anders, als dass man erst einmal personenbezogene Daten prinzipiell nicht nutzen darf, es sei denn, es gibt dafür eine Rechtsgrundlage (das ist selten, betrifft aber zum Beispiel Meldepflichten), oder aber der Betroffene gibt seine Erlaubnis dazu (das ist der Regelfall bei Datennutzung). Bei der Nutzung müssen folgende Punkte beachtet werden:

- Der Betroffene muss immer darüber informiert werden, welche seiner Daten erhoben und wozu sie benutzt werden.
- Der Betroffene hat dabei immer ein Widerspruchsrecht.
- Es dürfen generell nur diejenigen Daten genutzt werden, die für den Zweck erforderlich sind.
- Die Daten dürfen nur für den vorgesehenen Zweck verwendet werden. Der Zweck wird im Augenblick der Erhebung festgelegt. Zweckänderungen sind nicht zulässig.
- Es gilt das Ziel der Minimierung: Es sollen so wenig Daten wie möglich erfasst und gespeichert werden.
- Gespeicherte Daten müssen stimmen. Falsche oder veraltete Daten müssen gelöscht werden. Der Betroffene kann Aktualisierungen verlangen.
- Daten dürfen nur so lange gespeichert werden, wie sie für den Zweck, aus dem sie erhoben wurden, notwendig sind.

3. Die Pflichten im Datenschutz

3.1. Die Pflichten des Verantwortlichen

3.1.1. Einholen der Einwilligung

Für die Nutzung von persönlichen Daten benötigt man im Allgemeinen eine Einwilligung. Diese Einwilligung kann auch mündlich erfolgen, normalerweise wird jedoch eine Einwilligungserklärung aufgesetzt und unterschrieben.

3.1.2. Informationspflicht

Der Verantwortliche hat den Betroffenen immer zu informieren, welche Daten zu welchem Zweck gespeichert werden und auch über sein Widerspruchsrecht aufzuklären.

3.1.3. Maßnahmen zur Datensicherheit

Der Verantwortliche hat die Daten gegen den Zugriff Dritter zu schützen (Datensicherheit). Hierfür hat er technische und organisatorische Maßnahmen zu treffen. Zu den technischen Maßnahmen gehören z.B. Gebäudesicherung, IT-Sicherheit, Datenverschlüsselung, Passwortsicherheit, etc. Organisatorische Maßnahmen beziehen sich auf Handlungen, die vorgenommen werden müssen, z.B. das Wegschließen von Daten, das Sichern von Daten, das Verwenden sicherer Passwörter etc., auch Schulungen und Aufklärung der Mitarbeiter gehört dazu.

3.1.4. Datenschutz-Folgeabschätzung

Bei der Verarbeitung besonders sensibler Daten muss der Verantwortliche eine Datenschutzfolgeabschätzung erstellen. Dies ist ein spezielles Dokument, in dem die Risiken für Datenschutzverstöße ermittelt, sowie die daraus resultierenden Folgen für die Betroffenen abgeschätzt werden sollen.

3.2. Die Rechte des Betroffenen

Der Betroffene hat gegenüber dem Verantwortlichen folgende Rechte:

- *Auskunftsrecht*
  Der Betroffene hat jederzeit das Recht, sich darüber zu informieren, welche Daten über ihn gespeichert wurden. Die Auskunft hat zeitnah und kostenfrei zu erfolgen.
- *Recht auf Berichtigung*
  Der Betroffene hat ein Recht darauf, dass falsche Daten berichtigt werden.
- *Einschränkung und Löschung*
  Der Betroffene kann jederzeit verlangen, dass seine Daten gelöscht werden. Der Verantwortliche muss dann auch bei denjenigen Stellen auf ein Löschen der Daten hinwirken, an die er die Daten ggf. weitergegeben hat. Die Löschung muss dem Betroffenen bestätigt, nicht aber bewiesen werden.
- *Recht auf Übertragbarkeit*
  Bei einem Anbieterwechsel (neuer Stromanbieter, neue Arztpraxis) muss der alte Anbieter die Daten für den neuen Anbieter zur Verfügung stellen.
- *Widerspruchsrecht*
  Der Betroffene hat ein Widerspruchsrecht in Bezug auf die Nutzung von Daten. Dies ist aber kein generelles Widerspruchsrecht. Bei Datennutzung innerhalb eines Vertrages gelten vornehmlich die Vertragsbedingungen. Es gibt allerdings ein generelles Werbewiderspruchsrecht, dies kann vertraglich auch nicht ausgehebelt werden.
- *Sonstige Rechte*
  Der Betroffene hat das Recht darauf, dass automatisiert ermittelte Ergebnisse (z.B. bei Bewerbungen) noch einmal von einem Menschen kontrolliert werden. Dies würde auch für automatisiert ermittelte Diagnosen gelten, da hier der Arzt den Befund allerdings ohnehin bestätigen muss, gibt es hier keine Änderungen.

4. Datenschutz in der Arztpraxis

4.1. Die Maßnahmen der Praxis

4.1.1. Der Datenschutzbeauftragte

Da in einer Arztpraxis auf regelmäßiger Basis medizinische Daten verarbeitet werden, müsste streng genommen jede Praxis einen Datenschutzbeauftragten bestellen. Es hat sich jedoch durchgesetzt, dass dieser erst bindend wird, wenn 10 oder mehr Mitarbeiter (inklusive Arzt) Zugang zu empfindlichen Daten haben.

Die Kontaktdaten (z.B. Emailadresse) des Datenschutzbeauftragten müssen allen Betroffenen mitgeteilt werden. Der Name muss nicht mitgeteilt werden, es reicht eine Kontaktmöglichkeit. Die Kontaktdaten müssen weiterhin auch der Behörde gemeldet werden.

Der Datenschutzbeauftragte unterliegt einer „Verschwiegenheitspflicht“, und bei medizinischen Daten sogar der Schweigepflicht. Er dient als Ansprechpartner für Betroffene bei Fragen, Problemen und Bedenken.

Der Datenschutzbeauftragte darf betriebsintern benannt werden. Auch mehrere Beauftragte sind möglich. Der Datenschutzbeauftragte darf nicht gleichzeitig der Personalverantwortliche sein und die Aufgabe darf auch nicht vom (Praxis-)Chef übernommen werden. Ein betriebsinterner Datenschutzbeauftragter verfügt über einen gewissen Kündigungsschutz.

Der Datenschutzbeauftragte hat nur beratende Funktion. Er entbindet den Verantwortlichen nicht von irgendwelchen Pflichten oder Verantwortungen.

Die Aufgabe des Datenschutzbeauftragten ist vor allem für die Überwachung der Einhaltung der Datenschutzregelungen und die Unterrichtung, Beratung und Schulung des Verantwortlichen und der Mitarbeiter.

4.1.2. Die Einwilligungserklärung

In der Einwilligungserklärung stimmt der Betroffene der Nutzung seiner Daten durch den Verantwortlichen zu. Folgendes sollte bei der Einwilligungserklärung beachtet werden:

- Die Einwilligung muss nicht schriftlich erfolgen, aber die Nachweispflicht liegt beim Verantwortlichen. Daher ist die Schriftform ratsam.
- Die Einwilligung muss freiwillig erfolgen.
- Eine vorgelegte Einwilligungserklärung muss verständlich und klar als solche erkennbar sein.

- Eine Einwilligung kann auch unwirksam sein, wenn sie nicht den Vorgaben entspricht oder nicht angemessen ist.
- Man sollte sich keine Einwilligung holen, wo keine notwendig ist oder wo man sie nicht braucht.
- Einwilligungen können auch jederzeit widerrufen werden, darauf muss auch hingewiesen werden. Ein Kontakt für den Widerruf muss genannt werden.
- Die Einwilligung muss durch „aktives Handeln“ erfolgen. Der Hinweis auf ein Widerspruchsrecht allein ist keine Einwilligung.

4.1.3. Datenschutzfolgeabschätzung

Immer wenn bei der Verwendung von IT-Systemen hohe Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen, ist das Unternehmen verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen.

Eigentlich regelt die DSGVO, dass immer dann, wenn ein Datenschutzbeauftragter notwendig ist, auch eine DSFA vorhanden sein muss. Es hat sich jedoch durchgesetzt, dass in einer Arztpraxis eine Datenschutzfolgeabschätzung erwartet wird, auch wenn der Beauftragte erst ab 10 datenverarbeitenden Personen notwendig ist.

Eine Datenschutzfolgeabschätzung muss enthalten:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, inklusive des Zwecks der Verarbeitung.
- Eine Prüfung der Rechtmäßigkeit der Verarbeitung.
- Eine Bewertung der Notwendigkeit der Datenerhebung und Verarbeitung, sowie der Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.
- Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, Sicherheitsmaß-nahmen und Vorkehrungen. Mögliche Risiken können sein:
    - Diskriminierung
    - Identitätsdiebstahl
    - Finanzieller Verlust
    - Rufschädigung
    - Hinderung der Kontrolle über eigene Daten
    - Profilbildung mit Standortdaten

4.1.4. Verarbeitungsverzeichnis

Im Verarbeitungsverzeichnis werden alle Verarbeitungstätigkeiten aufgelistet, die in dem Unternehmen (in der Praxis) vorgenommen werden. Ein Verarbeitungsverzeichnis ist notwendig, wenn:

- besondere Risiken bestehen,
- die Verarbeitung regelmäßig erfolgt,
- es sich um besonders sensible Daten handelt,
- das Unternehmen mehr als 250 Mitarbeiter hat.

Da in einer Praxis auf regelmäßiger Basis persönliche Daten verarbeitet werden, ist ein Verarbeitungsverzeichnis notwendig. Im Verzeichnis wird Folgendes vermerkt:

- Eine allgemeine Beschreibung der (Praxis-)Organisation in Bezug auf Datenschutz.
- Die Dauer der Aufbewahrung.
- Ob Daten ins Ausland übertragen werden.

Man merkt hier schon, dass es Überschneidungen zur Datenschutzfolgeabschätzung gibt. Es ist immer möglich, in dem einen Dokument auf das andere Bezug zu nehmen.

4.2. Umgang mit medizinischen Daten

4.2.1. Datenschutz und Schweigepflicht

Die Schweigepflicht besteht in vollem Umfang weiter. Sie hat Vorrang vor dem Datenschutz und Verstöße werden auch strenger bewertet. Auch von der Schweigepflicht kann der Betroffene den Verantwortlichen prinzipiell entbinden. Dabei sind keine gesonderten Einwilligungen für Datenschutz und Schweigepflicht notwendig.

Unterschiede zwischen Datenschutz und Schweigepflicht bestehen in der Zuständigkeit. Für das Einhalten der Schweigepflichten ist der leitende Arzt zuständig, für den Datenschutz der Datenschutzbeauftragte.

Die Schweigepflicht entbindet nicht von gesetzlichen Meldepflichten.

4.2.2. Einsichtsrecht

Der Patient besitzt ein Einsichtsrecht für alle seine Daten und auch alle medizinischen Daten. Er kann also Einsicht in die Patientenakte verlangen. Früher waren persönliche Notizen und Anmerkungen vom Arzt über den Patienten ausgenommen, dies ist heute nicht mehr der Fall.

4.2.3. Umgang mit Praxissoftware

Jede datenverarbeitende Software ist ein potenzielles Risiko, dies gilt auch für die Praxissoftware. Generell gilt: Ein Softwareanbieter ist nie verantwortlich für Risiken oder Verstöße, die aus der Softwarenutzung ausgehen. Der Nutzer hat sich über Risiken zu informieren und diese dann zu minimieren.

4.3. Mögliche Konfliktfälle

4.3.1. Schutz von Dritten

In Einzelfällen kann es sein, dass ein Arzt seine Schweigepflicht und auch die Verpflichtung zum Datenschutz brechen muss. Dies kann zutreffen, wenn zum Beispiel Dritte gefährdet sind.

5. Kontrolle des Datenschutzes

5.1. Datenschutzverstöße

Ein Datenschutzverstoß bedeutet, dass persönliche Daten zugänglich gemacht wurden. Dabei spielt es keine Rolle, ob die Daten genutzt wurden oder ob ein Schaden entstanden ist. Ein Verstoß liegt bereits vor, wenn es Dritten möglich war, Einsicht zu nehmen.

Beispiele für Datenschutzverstöße sind:
- Verlust oder Diebstahl von Datenträgern mit persönlichen Daten
- Versenden eines Rundbriefes an Kunden mit offenen Adressen (cc. statt bcc.)
- Versenden von Emails mit persönlichen Daten an den falschen Adressaten
- Hackereinbrüche ins Firmennetz
- Datendiebstahl durch eigene Mitarbeiter
- Und vieles mehr…

5.2. Behördenkontrolle

Wie bei allen staatlichen Vorgaben können die Aufsichtsbehörden die Einhaltung des Datenschutzes kontrollieren. Bisher ist noch nicht viel von solchen Kontrollen bekannt. Dafür ist offensichtlich, dass die Aufsichtsbehörden für flächendeckende Routinekontrollen personell überhaupt nicht ausgestattet sind. Das Risiko einer Routinekontrolle ist also gering, Probleme machen eher die Anzeige von erfolgten oder angenommenen Verstößen, denen die Behörde nachgehen muss.

5.3. Selbstkontrolle

Zur Selbstkontrolle dient in einem Unternehmen (falls vorhanden) der Datenschutzbeauftragte. Dabei gehört zu den Pflichten des Datenschutzbeauftragten, jeden Verstoß gegen den Datenschutz der Behörde zu melden. Natürlich müssen auch Unternehmen ohne Datenschutzbeauftragten solche Verstöße melden. Die Meldung soll innerhalb von 72 Stunden erfolgen, viele Behörden haben hierfür Portale eingerichtet.

5.4. Strafen

5.4.1. Behördliche Strafen

Die Behörde darf bei Datenschutzverstößen Bußgelder verhängen. Ab welcher Größe des Verstoßes und in welcher Höhe ist noch weitgehend ungeklärt. Vorgesehen sind hierfür 2-4% des Jahresumsatzes. Bußgelder werden aber mutmaßlich eher die Ausnahme bleiben. Gründe für den Datenschutz sind eher Image-Verlust bzw. Klagen von Kunden.

5.4.2. Schadenersatzklagen

Bei Verstößen kann der Betroffene, dessen Daten falsch behandelt wurden, auf Schadenersatz klagen. Um aber Schadenersatz zu erhalten, muss ein entstandener Schaden nachgewiesen sein. Der Verstoß allein reicht nicht aus, er muss auch schädliche Folgen gehabt haben.

5.4.3. Straffreiheit

Der Verantwortliche kann nicht bestraft werden, wenn er für einen Verstoß nicht verantwortlich gemacht werden kann. Werden zum Beispiel Daten trotz angemessener Sicherheitsmaßnahmen gestohlen und missbraucht, so kann der Verantwortliche nicht verurteilt werden.

6. Anhang

6.1. Glossar

Ärztliche Schweigepflicht
Die Ärztliche Schweigepflicht ist „strenger“ als der normale Datenschutz. Bei Patient und Arzt wird ein besonderes Vertrauensverhältnis vorausgesetzt.

Datensicherungen
Das Speichern von Daten auf einem zweiten Speichermedium, um vor Datenverlust bei technischen Pannen zu schützen. Datensicherungen werden vorausgesetzt. Verursacht ein Dienstleister (z.B. bei einer technischen Wartung) einen Datenverlust, so kann der entstandene Schaden nicht vom Dienstleister eingeklagt werden.

Natürliche Person
Ein Mensch aus Fleisch und Blut. Eine juristische Person kann auch eine Firma sein.

6.2. Abkürzungen

DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutzgrundverordnung
EU-DSGV	Europäische Datenschutzgrundverordnung

6.3. Einige Fragen zum Datenschutz

Bin ich verantwortlich für die Sicherheit beim Versand von Daten, die mir geschickt werden?
Nein, ich bin nur für die Sicherheit des Versandes verantwortlich, wenn ich die Daten selbst verschicke. Beispiel: Schickt ein Patient sensible Daten über eine unverschlüsselte Email an die Arztpraxis, so ist das seine eigene Verantwortung. Antwortet die Praxis aber auf diese Email, und die sensiblen Daten stehen im Mailverlauf, so ist das in dem Augenblick ein Verstoß, wenn die Mail nicht entsprechend gesichert wurde.

Gilt der Datenschutz auch noch nach dem Tod des Betroffenen?
Prinzipiell ja. Das Recht geht sozusagen auf die Erben über. Entscheidend ist auch der Wille des Verstorbenen. Darin kann Datenübertragung und Datenlöschung verlangt werden.