Die Datenschutz-Grundverordnung tritt in Kraft – das müssen selbstständige Heilberufler beachten

https://uldsh.de/dsgvo-aerzte, Stand: 25. Mai 2018

Am 25. Mai 2018 tritt die im Jahr 2016 verabschiedete EU-Datenschutz-Grundverordnung (DSGVO) vollständig in Kraft. Sie wird dann die wesentlichen in Deutschland und den anderen EU-Mitgliedstaaten anzuwendenden Vorschriften über den Datenschutz enthalten. Ergänzend finden sich für Heilberufler einzelne Konkretisierungen im neuen Teil 2 des Bundesdatenschutzgesetzes (BDSG), das am gleichen Tag in Kraft tritt.

Wer ist Verantwortlicher?

Der Betreiber oder die Betreiberin der Praxis, Apotheke etc. ist die oder der **Verantwortliche** im Sinne des Gesetzes. Sie oder er hat sicherzustellen, dass die Vorschriften über den Datenschutz eingehalten werden. Dazu gehört die Pflicht, bestimmte Dokumentationen zu führen, mit denen die Einhaltung der Vorgaben nachgewiesen werden kann.

In diesem Text sollen die wichtigsten Anforderungen der DSGVO und des BDSG für selbstständige Heilberufler kurz vorgestellt werden. Dabei wird auch auf bereits vorhandene Informationsquellen verwiesen, insbesondere auf die „Kurzpapiere“ die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu einer Reihe von wichtigen Themen und Begriffen des neuen Rechts gemeinsam entwickelt und veröffentlicht hat.

Rechtsgrundlagen für die Verarbeitung personenbezogener Daten der Patienten: Vertrag oder Einwilligung

Die DSGVO erlaubt die Verarbeitung von personenbezogenen Daten nur, wenn dafür eine **Rechtsgrundlage** zur Verfügung steht.

Im Fall einer Arztpraxis, Apotheke etc. ist die Rechtsgrundlage **in der Regel der Vertrag**, der mit dem Patienten geschlossen wird. Die zur Begründung, Durchführung und Beendigung des Vertrags notwendigen Daten dürfen verarbeitet werden.

Dazu gehören in der Arztpraxis z.B. Name, Anschrift, Versicherungsnummer des Patienten, die ärztliche Dokumentation von Anamnese und Behandlung, Arztbriefe, Laborberichte.

Soweit **zusätzliche Dienste** angeboten werden, wie z.B. ein Recall-Service, kann die Verarbeitung von personenbezogenen Daten für diesen Zweck nicht auf den Behandlungsvertrag gestützt werden. Hier ist die **Einwilligung** des Betroffenen einzuholen.

Die Einwilligung muss nicht zwingend schriftlich eingeholt werden. Im Zweifel muss der Arzt etc. allerdings nachweisen, dass die Einwilligung gegeben wurde. Dazu eignet sich ein unterschriebenes Formular am besten.

Auch für die Weitergabe der Daten von Privatpatienten an die PVS oder eine andere **private Verrechnungsstelle** ist die Einwilligung der Patienten bzw. eine Schweigepflichtsentbindungserklärung erforderlich. Dies gilt jedenfalls dann, wenn es zur Abtretung der Honorarforderung kommt.

Auch die teilweise praktizierte Bonitätsüberprüfung von potentiellen Privatpatienten mittels Auskunfteien wie der Schufa ist nur mit der Einwilligung der Betroffenen zulässig.

Wenn **mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen** oder behandeln, kann nach § 9 Abs. 4 der Berufsordnung der Ärztekammer SH angenommen werden, dass die Patienten damit einverstanden sind, dass diese Ärzte untereinander Informationen austauschen. Allerdings müssen dafür wenigstens **Anhaltspunkte** vorliegen, die auch dokumentiert werden müssen. Dies ist z.B. der Fall, wenn ein Patient den Namen seines Hausarztes nennt. Werden medizinische Informationen z.B. von einem Krankenhaus an ein MVZ weitergegeben, in welchem die Patientin noch nie in Behandlung war, nur weil das Krankenhaus regelmäßig mit dem MVZ zusammenarbeitet, liegt keine zulässige Weitergabe der Daten an nachbehandelnde Ärzte vor.

Die **Wirksamkeit der Einwilligung** eines Patienten in die Weitergabe seiner Patientendaten an Dritte („Schweigepflichtentbindungserklärung“) setzt weiterhin voraus, dass dieser ausreichende Informationen über Identität und Kontaktdaten der Empfänger, den Zweck und den Umfang der beabsichtigten Datenübermittlung erhält. Zudem muss der Patient darüber aufgeklärt werden, dass die Abgabe der Einwilligung freiwillig ist und welche Folgen eine Verweigerung oder ein Widerruf der Einwilligung hat.

Informationspflichten: Die Betroffenen müssen über bestimmte Umstände bei der Verarbeitung ihrer Daten informiert werden (Art. 13 DSGVO).

Die Informationspflicht soll die **Transparenz** bei der Verarbeitung personenbezogener Daten fördern. Nur wenn jemand weiß, dass Daten über ihn oder sie verarbeitet werden und welche Rechte er oder sie dabei hat, können diese Rechte auch wahrgenommen werden.

Vor allem die **folgenden Informationen** müssen den Patienten in Arztpraxen etc. gegeben werden:

- Namen und Kontaktdaten des Verantwortlichen;
- die Kontaktdaten des Datenschutzbeauftragten, falls einer benannt wurde (dazu siehe unten);
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- die Dauer, für die die personenbezogenen Daten gespeichert;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf einer Einwilligung beruht, das Bestehen eines Rechts, die Einwilligung jederzeit für die Zukunft zu widerrufen;
- das Bestehen eines Beschwerderechts bei der Datenschutzaufsichtsbehörde, also in Schleswig-Holstein bei dem Unabhängigen Landeszentrum für Datenschutz;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte.

Werden die Daten nicht direkt beim den Betroffenen, sondern bei Dritten erhoben, so muss zusätzlich mitgeteilt werden,

- um welche Kategorien von Daten es sich handelt und
- aus welchen Quellen diese Daten stammen.

Diese Informationen müssen den Patienten im **zeitlichen Zusammenhang mit der Erhebung der Daten** zur Verfügung gestellt werden.

Dies geschieht am einfachsten z.B. mit einem **Flyer oder Handzettel**, der an die Patienten bei der Aufnahme ausgegeben wird. Es genügt auch, wenn der Zettel nur die wichtigsten Informationen zusammenfasst und im Übrigen auf die Homepage der Praxis verweist, wo sich die Einzelheiten finden lassen.

Der oder die Verantwortliche muss die **Erfüllung der Informationspflicht nachweisen** können. Dazu ist es z.B. ausreichend, wenn den Patienten standardmäßig bei der Aufnahme der Zettel übergeben wird und dies für jeden Patienten im Praxissystem vermerkt wird. Es ist nicht erforderlich, dass die Patienten mit ihrer Unterschrift quittieren, dass sie die Informationen erhalten haben.

Ebenso wenig ist es erforderlich, den Patienten die Informationen schon am Telefon vorzulesen, wenn diese anrufen, um einen Termin zu vereinbaren. Hier genügt es, wenn die Informationen auf der Homepage der Praxis leicht auffindbar sind. Nicht ausreichend wäre es andererseits, wenn die Informationen lediglich in der Praxis ausgehängt werden.

Die Bundesärztekammer hat angekündigt, eine Musterinformation für Arztpraxen zu erstellen.

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Als einen wichtigen Baustein zur Dokumentation der beim Verantwortlichen stattfindenden Verarbeitung personenbezogener Daten verlangt die DSGVO, dass der Verantwortliche ein „Verzeichnis der Verarbeitungstätigkeiten“ führt. Dieses tritt an die Stelle des nach altem Recht bekannten Verfahrensverzeichnisses.

Zu beachten ist, dass in das neue Verzeichnis auch solche „**Verarbeitungstätigkeiten**“ aufgenommen werden müssen, die nur teilweise automatisiert oder sogar gänzlich manuell durchgeführt werden.

Das Kurzpapier Nr. 1 enthält weitere Erläuterungen zum Inhalt des Verzeichnisses.

Das **ULD hat ein Muster für die Beschreibung einer Verarbeitungstätigkeit bereitgestellt**. Die Verantwortlichen müssen dann eine solche Beschreibung für alle von ihnen ausgeführten Verarbeitungstätigkeiten erstellen und sammeln. Diese Sammlung ist das Verzeichnis der Verarbeitungstätigkeiten. Anders als sein Vorgänger, das Verfahrensverzeichnis, ist es nicht mehr zur Veröffentlichung bestimmt.

Muss ein betrieblicher Datenschutzbeauftragter benannt werden?

Nach § 38 Bundesdatenschutzgesetz (BDSG) ist ein **betrieblicher Datenschutzbeauftragter** (DSB) in jedem Fall dann zu bestellen, wenn in der Arztpraxis, Apotheke etc. **in der Regel mindestens zehn Personen** ständig, d.h. nicht nur gelegentlich, **mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt** sind. In einer Arztpraxis zählen zu diesen Personen zunächst die Ärzte selbst, da sie im Hinblick auf ihre Dokumentationspflicht medizinische Daten über die Betroffenen zu verarbeiten haben. Zu den mit der automatisierten Verarbeitung befassten Personen gehört auch medizinisches Hilfspersonal, soweit es die Daten der Patienten verarbeitet. Dies gilt z.B. für Arzthelfer etc., die Laborwerte, Ergebnisse von Tests etc. oder auch Termine in das Praxissystem eingeben. Mitzuzählen sind auch Verwaltungskräfte, die die Abrechnung organisieren oder Daten über die Mitarbeiter der Praxis pflegen. Nicht mitzuzählen sind dagegen z.B. Reinigungskräfte, die normalerweise keinen Zugriff auf die Daten haben.

Die **DSGVO nennt noch weitere Konstellationen**, bei deren Vorliegen ein betrieblicher DSB zu benennen ist. Von Bedeutung ist hier vor allem der Fall, dass zur Kerntätigkeit des Verantwortlichen die **Verarbeitung von Gesundheitsdaten in großem Maßstab** gehört. Zwar wird man im Hinblick auf die Bedeutung der Dokumentation und der Verwaltung von Patientendaten davon ausgehen können, dass die Verarbeitung solcher Daten zur Kerntätigkeit in Arztpraxen, Apotheken etc. gehört. Allerdings wird in den allermeisten Fällen nicht von einer Verarbeitung in großem Maßstab auszugehen sein.

Etwas anderes gilt nur in besonders gelagerten Fällen, in denen der Umfang der Verarbeitung von Gesundheitsdaten (oder anderen sensiblen Daten wie z.B. genetischen Daten) weit über das hinausgeht, was in einer üblichen Arztpraxis anzutreffen ist. In einem solchen Fall ist die Benennung eines betrieblichen DSB verpflichtend.

Ist ein betrieblicher DSB zu benennen, so kommen neben **eigenem Personal** auch **externe DSB** in Betracht. Wichtig ist vor allem, dass der DSB die notwendige Fachkunde zu Datenschutzrecht und –praxis besitzt oder sich in kurzer Zeit verschafft. U.a. bietet die DATENSCHUTZAKADEMIE SH Fortbildungen für die betrieblichen DSB an.

Die **Kontaktdaten des betrieblichen DSB sind zu veröffentlichen** und der zuständigen **Aufsichtsbehörde mitzuteilen**. Hier geht es zu dem **Meldeformular des ULD**.

Weitere Informationen zur Benennung von Datenschutzbeauftragten finden sich im Kurzpapier Nr. 12.

Muss eine Datenschutz-Folgenabschätzung durchgeführt werden?

Die DSGVO sieht vor, dass vor dem Einsatz von bestimmten, für die Rechte der Betroffenen **besonders riskanten Verfahren** eine „Datenschutz-Folgenabschätzung" (englisch: „Data protection impact assessment") durchzuführen ist. Damit soll der Grad der Gefährdung genauer bestimmt und festgestellt werden, ob hinreichende Schutzmechanismen getroffen worden sind.

Eine Datenschutz-Folgenabschätzung ist nach der DSGVO unter anderem dann erforderlich, wenn **Gesundheitsdaten in großem Maßstab verarbeitet** werden. Dies trifft zum Beispiel auf Krankenhäuser, MVZ, stationäre Pflegeeinrichtungen, ggf. ambulante Pflegedienste oder medizinische Abrechnungsdienste zu.

Bei kleinen und mittelgroßen Arztpraxen, Apotheken etc. ist allerdings nicht von einer Verarbeitung von Gesundheitsdaten in großem Maßstab auszugehen. Daher wird eine Datenschutz-Folgenabschätzung hier regelmäßig nicht erforderlich sein.

Etwas anderes gilt – wie bei der Benennung von betrieblichen Datenschutzbeauftragten – nur in besonders gelagerten Fällen, in denen der Umfang der Verarbeitung von Gesundheitsdaten (oder anderen sensiblen Daten wie z.B. genetischen Daten) weit über das hinausgeht, was in einer üblichen Arztpraxis anzutreffen ist. In einem solchen Fall ist eine Datenschutz-Folgenabschätzung durchzuführen.

Weitere Informationen zur Durchführung einer Datenschutz-Folgenabschätzung finden sich im Kurzpapier Nr. 5 sowie in dieser Veröffentlichung des Forums Privatheit.

Weitere Pflichten

Wie schon bisher sind auch die **allgemeinen Pflichten aus dem Datenschutzrecht** beachten. Dazu gehört vor allem:

- die **Beschränkung der Datenverarbeitung** auf das erforderliche Maß;
- die **fristgerechte Löschung** von Daten (in Arztpraxen in der Regel, nachdem die zehnjährige Aufbewahrungsfirst abgelaufen ist);
- die Einhaltung von **technisch-organisatorischen Maßnahmen**, mit denen unter anderem der Zugriff Unbefugter auf die Daten verhindert wird;
- auf Antrag der Betroffenen die **Gewährung von Auskunft** über die zu ihrer Person verarbeiteten Daten, dazu Kurzpapier Nr. 6;
- Abschluss von **Verträgen** mit Stellen, die **Daten im Auftrag** der Praxis etc. verarbeiten (z.B. IT-Dienstleistern), dazu Kurzpapier Nr. 13;
- die **Meldung von Datenschutzvorfällen** an die Datenschutz-Aufsichtsbehörde und gegebenenfalls Benachrichtigung an die Betroffenen nach Art. 33 und 34 DSGVO (hierzu werden noch detailliertere Informationen bereitgestellt).

Um zu überprüfen, ob diese Vorgaben eingehalten werden, empfehlen wir, den vom ULD für Arztpraxen entwickelten Selbstcheck auf Ihre Praxis anzuwenden.

Ein Überblick über die Pflichten für Arztpraxen findet sich auch auf einem Merkblatt der Bundesärztekammer.