Landespsychotherapeutenkammer Baden-Württemberg

EU-DATENSCHUTZ-GRUNDVERORDNUNG TRITT AM 25.05.2018 IN KRAFT- WICHTIGE INFORMATIONEN FÜR PRAXISINHABER

Am 25.05.2018 tritt die neue europäische Datenschutz-Grundverordnung (2016/679, EU-DSGVO) in Kraft (zum Text der Verordnung: hier). Diese dient der Vereinheitlichung des europäischen Datenschutzrechtes.

Die EU-DSGVO gilt für die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen** (Art. 2 DSGVO). Dabei stellen auch Karteisysteme zur Verwaltung von Patientendokumentationen, bei denen die Patientenakten nach festgelegten Ordnungskriterien abgelegt werden, ein Dateisystem im Sinne der EU-DSGVO dar, sodass auch für diese die EU-DSGVO Anwendung findet. Der datenschutzrechtliche Begriff des „**Verarbeitens**" ist weit auszulegen, denn hierunter fallen alle Tätigkeiten, bei denen personenbezogene Daten erhoben, erfasst, geordnet, gespeichert, geändert , abgerufen, zugänglich gemacht, übermittelt oder vernichtet werden (Art. 4 Nr. 2 DSGVO). **Personenbezogene Daten** sind sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Patienten, Bezugspersonen) beziehen (Art. 4 Nr. 1 DSGVO). Aus den vorgenannten Gründen ist die EU-DSGVO bei der Verarbeitung personenbezogener Daten in den Psychotherapiepraxen bindend und zu beachten. Neben der EU-DSGVO sind bei der Verarbeitung personenbezogener Daten das Bundesdatenschutzgesetz (BDSG) und die einschlägigen Fachgesetze (bspw. Sozialgesetzbuch Teil 5- SGB V) zu beachten.

Mit dem Inkrafttreten sämtlicher Regelungen der EU-DSGVO ändert sich die Rechtslage zur Verarbeitung personenbezogener Daten im Vergleich zum vorherigen Recht. Die im BDSG und den einschlägigen Fachgesetzen verankerten Grundsätze zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Rechtmäßigkeitsprinzip, Prinzip der Zweckbindung und der Datensparsamkeit) gelten weitestgehend fort. Allerdings sind **mit der EU-DSGVO weitergehende Pflichten für die im datenschutzrechtlichen Sinne Verantwortlichen verbunden, deren Nichterfüllung Sanktionen nach sich ziehen kann.**

Wir geben Ihnen im Folgenden einige einführende Informationen, um Sie auf die wesentlichen Neuerungen und Besonderheiten hinzuweisen. Außerdem geben wir Ihnen unverbindliche Empfehlungen sowie Links zu Mustern, die Ihnen als Grundlage der vorzunehmenden Anpassungen in Ihrer Praxis dienen können. Es wird anwaltliche Beratung oder Hinzuziehung eines Datenschutzbeauftragten empfohlen.

1. Verantwortliche für die Umsetzung in der Praxis

Für die Einhaltung der Vorgaben der EU-DSGVO, des BDSG und der einschlägigen Fachgesetze sind grundsätzlich der oder die Praxisinhaber verantwortlich (Art. 4 Nr. 7 DSGVO), gegebenenfalls unterstützt durch einen betrieblichen Datenschutzbeauftragten.

Den oder die Verantwortlichen für die Umsetzung der EU-DSGVO, des BDSG und der datenschutzrechtlichen Regelungen in den Fachgesetzen **treffen ab dem 25. Mai 2018 weiterreichende Rechenschafts-, Informations- und Nachweispflichten, deren Nichteinhaltungen als Ordnungswidrigkeit verfolgt und mit Bußgeldern belegt oder zivilrechtliche Schadenersatzforderungen nach sich ziehen können.**

Aus diesem Grund empfiehlt die Landespsychotherapeutenkammer Baden-Württemberg allen Praxisinhabern, sich über die erforderlichen Anforderungen zu informieren und diese unverzüglich in den Praxen umzusetzen.

2. Pflichten für die verantwortlichen Praxisinhaber und Empfehlungen der Kammer

Wie nach bisherigem Recht auch, ist die **Verarbeitung von personenbezogenen Daten nur dann zulässig, wenn entweder eine Rechtsgrundlage diese ausdrücklich gestattet oder aber der Betroffene seine Einwilligung zur Verarbeitung seiner personenbezogenen Daten erteilt hat** (Rechtmäßigkeitsprinzip). Die bei der Anbahnung eines Behandlungsverhältnisses und bei der Durchführung der Behandlung üblicherweise anfallenden Datenverarbeitungsvorgänge sind in den meisten Fällen durch Art. 9 Abs. 2 lit. h DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. b BDSG sowie durch die Vorschriften der speziellen Fachgesetze (insbesondere SGB V) legitimiert. In den anderen Fällen ist eine Einwilligung des Betroffenen, bzw. bei einwilligungsunfähigen Patienten des gesetzlichen Vertreters, erforderlich. Die Einwilligung kann grundsätzlich mündlich erteilt werden, es sei denn, die Schriftform wird ausdrücklich angeordnet (bspw. bei der Befundübermittlung der Vertragspsychotherapeutinnen und –psychotherapeuten an die Hausärzte gem. § 73 Abs. 1 b SGB V). Einwilligungsformulare sollten überprüft und auf einen neuen Stand gebracht werden, insbesondere sind die Patienten auf ihr Recht zum Widerruf der Einwilligung hinzuweisen.

Die EU-DSGVO schreibt umfassende **Informationspflichten** für die bei der Verarbeitung personenbezogener Daten Verantwortlichen vor. Werden personenbezogene Daten direkt bei den Patienten erhoben, so sind die in Art. 13 DSGVO geregelten Informationen im Zeitpunkt der Datenerhebung dem Patienten mitzuteilen, insbesondere die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung. Erfolgt die Erhebung bei einem Dritten (bspw. durch Beiziehung von Befunden), so sind die in Art. 14 DSGVO genannten Informationen in angemessener Zeit dem Patienten mitzuteilen. Weiterhin sind dem Patienten die in Art. 13, 14 DSGVO genannten zusätzlichen Informationen zur Verfügung zu stellen. Es empfiehlt sich, ein **standardisiertes Formular** zu erarbeiten, welches dem Patienten ausgehändigt werden kann (zur Mitteilung von Informationen) und einen deutlich sichtbaren **Aushang in der Praxis** anzubringen, mit dem die zusätzlichen Informationen zur Verfügung gestellt werden. Ein Muster finden Sie weiter unten unter der Überschrift „4. weiterführende Informationen und Links“.

Haben Sie eine Praxiswebseite, so müssen Sie ab dem 25. Mai 2018 auch bei der **Gestaltung dieser Webseite die Vorgaben der DSGVO umsetzen**, da beim Zugriff auf diese Webseite (allgemeiner Zugriff, Kontaktformulare, E-Mailkorrespondenz) in der Regel automatisiert personenbezogene Daten verarbeitet werden. Den Informationspflichten ist durch Erstellung einer korrekten **Datenschutzerklärung** auf der Praxiswebseite Rechnung zu tragen. Ein Muster finden Sie weiter unten unter der Überschrift „4. weiterführende Informationen und Links“. Dieser sollte besondere Sorgfalt gewidmet werden, da auch eine fehlende oder unvollständige Datenschutzerklärung auf einer öffentlich zugänglichen Webseite leicht feststellbar ist und zu Sanktionen führen kann.

Haben Sie einen Vertrag mit einem externen Dienstleister o.ä. abgeschlossen, bei dem der dieser Zugriff auf personenbezogene Daten erhalten kann (bspw. EDV-Fernwartung) oder werden personenbezogene Daten in Ihrem Auftrag von einem Dritten verarbeitet (gespeichert, vernichtet usw.), so empfehlen wir Ihnen, mit diesem Dienstleister einen **Auftragsdatenverarbeitungsvertrag (ADV)** abzuschließen, um somit eine datenschutzrechtliche Legitimationsgrundlage für den Drittzugriff zu schaffen. Der ADV muss den Anforderungen des § 11 BDSG Genüge tun. Sie müssen den Auftragsdatenverarbeiter sorgfältig ausgewählt haben und durch die vertragliche Vereinbarung sicherstellen, dass dieser nur im Rahmen des Erforderlichen und nur im Rahmen Ihrer Weisungen Zugriff erhalten kann. Ein Muster finden Sie weiter unten unter der Überschrift „4. weiterführende Informationen und Links“. Ungeachtet dessen müssen Berufsgeheimnisträger bei Verträgen mit externen Dienstleistern aufgrund der Anforderungen des § 203 Abs. 4 S. 2 Nr. 1 Strafgesetzbuch zur Vermeidung einer Strafbarkeit die **mitwirkenden Dienstleister zusätzlich zur Geheimhaltung verpflichten**. Es sollten deshalb alle bestehenden Verträge mit externen Dienstleistern geprüft und an die neuen rechtlichen Anforderungen angepasst werden.

Bei der Verarbeitung personenbezogener Gesundheitsdaten, als besonders sensiblen Daten, werden erhöhte Anforderungen an die Rechtmäßigkeit der Verarbeitung gestellt. Die DSGVO schreibt vor, dass bei der Verarbeitung personenbezogener Gesundheitsdaten ein **Verzeichnis von Verarbeitungstätigkeiten zu führen** ist (Art. 30 DSGVO), in welchem die Datenverarbeitungsprozesse schriftlich dokumentiert sind und welches auf Verlangen der zuständigen Aufsichtsbehörde für den Datenschutz zur Verfügung gestellt werden muss. Ein Muster finden Sie weiter unten unter der Überschrift „4. weiterführende Informationen und Links“.

Weiterhin schreibt die DSGVO vor (Art. 35), dass eine **datenschutzrechtliche Folgenabschätzung** verpflichtend vorzunehmen ist, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs oder der Umstände und der Zwecke ein voraussichtlich hohes Risiko für die Rechte der Betroffenen hat. Allerdings werden die Kriterien zur Bestimmung der Notwendigkeit nicht eindeutig definiert. Die DSGVO statuiert lediglich, dass insbesondere bei der Anwendung neuer Technologien im IT-Bereich (bspw. Nutzung von Cloud Speichern), bei der Videoüberwachung öffentlicher Bereiche und bei der „umfangreichen Verarbeitung von Gesundheitsdaten“ ein erhöhtes Risiko besteht, welches die datenschutzrechtliche Einschätzung der Folgen der Datenverarbeitung obligat macht. Wann jedoch „umfangreiche Verarbeitung von Gesundheitsdaten“ vorliegen soll, wird nicht definiert. Aus diesem Grund kann die Landespsychotherapeutenkammer zum jetzigen Zeitpunkt keine Auskunft darüber treffen, ob und unter welchen Voraussetzungen eine solche Verpflichtung zur Vornahme einer Datenschutz-Folgenabschätzung für Psychotherapie-Praxen tatsächlich besteht. Ein Muster finden Sie weiter unten unter der Überschrift „4. weiterführende Informationen und Links“. Da sich Psychotherapiepraxen von der Anzahl der Patienten und der Größe der Praxis wesentlich von den meisten Arztpraxen unterscheiden, kann man eine sogenannte „umfangreiche Verarbeitung von Gesundheitsdaten“ zumindest in Frage stellen. Wir empfehlen eine Einschätzung für Ihre Praxis unter Angabe der Einzelheiten (Anzahl der Patienten, Anzahl der Mitarbeiter in der Praxis, Umfang der verarbeiteten Daten) beim Landesdatenschutzbeauftragten einzuholen. Die LPK BW wird zeitgleich eine allgemeine Anfrage beim Landesdatenschutzbeauftragten zu psychotherapeutischen Praxen stellen und über das Ergebnis informieren.

Darüber hinaus besteht eine **Rechtspflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten**, wenn in einer Praxis mehr als 9 Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst werden (§ 38 Abs. 1 BDSG). Allerdings dürfte dieses Kriterium auf Psychotherapiepraxen regelmäßig nicht zutreffen. Wir müssen in diesem Zusammenhang aber darauf hinweisen, dass ungeachtet der Anzahl der mit der Verarbeitung personenbezogener Daten befasster Mitarbeiter auch dann ein betrieblicher Datenschutzbeauftragter zu bestellen ist, wenn die Voraussetzungen zur Vornahme einer Datenschutz-Folgenabschätzung (s.o.) vorliegen. Aufgrund der aufgezeigten

Rechtsunsicherheiten ist deshalb eine allgemeine Abklärung beim Landesdatenschutzbeauftragten sinnvoll.

Außerdem räumt die DSGVO den Patienten ein allgemeines **Auskunftsrecht** (Art. 15 DSGVO) über sämtliche ihn betreffenden personenbezogenen Daten gegen den Verantwortlichen ein. Die Auskunft ist dem Patienten grundsätzlich unverzüglich und unentgeltlich zu erteilen. Dieses Auskunftsrecht ist jedoch von dem Recht auf Einsichtnahme in die Patientendokumentation (§ 630g BGB, § 11 Berufsordnung) zu unterscheiden. Während sich das Auskunftsrecht des Art. 15 DSGVO lediglich auf eine allgemeine Information zum Umfang der verarbeiteten personenbezogenen Daten bezieht, geht es bei der Einsichtnahme in die Dokumentation um die Kenntnisnahme des fachlichen Inhalts der Patientenakte.

Weiterhin haben Patienten einen Anspruch auf **Löschung personenbezogener Daten**, wenn und soweit die gesetzlichen und berufsrechtlichen Pflichten zur zehnjährigen Aufbewahrung der Behandlungsdokumentation dem nicht entgegenstehen (§ 35 Abs. 3 BDSG i.V.m. § 630f BGB, 11 Berufsordnung). Nach Ablauf der zehnjährigen Aufbewahrungsfrist sind die personenbezogenen Daten auf Verlangen des Patienten grundsätzlich zu löschen, es sei denn, dass diese für die weitere Aufgabenerfüllung oder die eigene Rechtsverfolgung (bspw. im Rahmen von Gerichtsprozessen) noch zwingend erforderlich sind. Auch ohne ein ausdrückliches Verlangen des Patienten müssen Praxisinhaber nach Ablauf der gesetzlichen und satzungsrechtlichen Aufbewahrungsfrist nach den allgemeinen Grundsätze der Erforderlichkeit und Datensparsamkeit prüfen, ob die personenbezogenen Daten für die (weitere) Aufgabenerfüllung der verantwortlichen Stelle noch benötigt werden. Werden diese absehbar nicht mehr benötigt, so sollte eine datenschutzkonforme Löschung erfolgen.

Im Falle etwaiger datenschutzrechtlicher Verstöße (bspw. Diebstahl eines Laptops, auf dem personenbezogene Daten von Patienten gespeichert sind) sind die **zuständige Aufsichtsbehörde für den Datenschutz zu informieren** und der oder die betroffenen **Patienten zu benachrichtigen**.

Im Übrigen gelten weiterhin die **allgemeinen datenschutzrechtlichen Pflichten**, sodass die technischen Standards zur Wahrung des Datenschutzes zu beachten sind. Als Orientierung zur Beurteilung der technischen Anforderungen an datenschutzkonforme Verarbeitungsvorgänge kann die technische Anlage der Bundesärztekammer zur Schweigepflicht dienen, siehe unten unter „4. Weiterführende Informationen und Links“, welche jedoch aktuell überarbeitet und an die neue Rechtslage angepasst wird.

3. Zuständige Aufsichtsbehörde für den Datenschutz

Zuständig für die Überwachung der Einhaltung des Datenschutzes ist der Landesbeauftragte für Datenschutz in Baden-Württemberg:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg
Königstraße 10 a
70173 Stuttgart

https://www.baden-wuerttemberg.datenschutz.de/

4. Weiterführende Informationen und Links zu Mustern und Leitfäden:

Zu Ihrer weiteren Information verweisen wir auf:

1. Die Hinweise und Muster auf der Homepage der Kassenärztlichen Bundesvereinigung:

   http://www.kbv.de/html/datensicherheit.php

2. Die Hinweise und Muster auf der Homepage der Landeszahnärztekammer Baden-Württemberg:

   https://lzk-bw.de/zahnaerzte/praxisfuehrung/eu-datenschutz-grundverordnung/

3. Die Hinweise auf der Homepage des Landesdatenschutzbeauftragten Baden-Württemberg inklusive Muster eines Auftragsdatenverarbeitungsvertrages (ADV):

   https://www.baden-wuerttemberg.datenschutz.de/ds-gvo/

   https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfen-merkblatter/

4. Die Hinweise und Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zur Schweigepflicht, Datenschutz und Datenverarbeitung in der Praxis:

   http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf

   http://www.kbv.de/media/sp/Checkliste_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

   http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Telemedizin_Telematik/Sicherheit/Schweigepflicht_Technische_Anlage_2008.pdf

Wie Sie sehen, sind noch viele Fragen offen, die erst im Laufe der Zeit von den zuständigen Aufsichtsbehörden und durch die Gerichte zu klären sind. Aus diesem Grund erheben die hier eingestellten Informationen keinen Anspruch auf Vollständigkeit und Richtigkeit. Eine Haftung der Landespsychotherapeutenkammer für die eingestellten Informationen kann nicht übernommen werden. Für Einzelfragen werden Sie gebeten, sich an die o.g. zuständige Behörde für den Datenschutz zu wenden.