Hinweise zur Europäischen Datenschutz-Grundverordnung (EU-DSGVO)

Ab dem 25.5.2018 gilt in der Europäischen Union die EU-Datenschutzgrundverordnung (EUDSGVO) unmittelbar in jedem Mitgliedsland als neues und gegenüber dem nationalen Recht vorrangiges Datenschutzrecht. Auch wenn das deutsche Datenschutzrecht schon bisher eines der strengsten war und Europa sich jetzt teilweise den in Deutschland bereits geltenden Standards anpasst, sollte die EUDSGVO den Arztpraxen Anlass dazu geben, sich mit dem Thema Datenschutz eingehend zu beschäftigen. Dies allein schon deshalb, weil ab dem 25.5.2018 deutlich schärfere Bußgeldvorschriften gelten: Das Bußgeld kann – auch wenn der Höchstwert für Arztpraxen nicht zum Tragen kommen dürfte – bis zu 20 Mio. Euro bzw. 4 v. H. des Jahresumsatzes (je nachdem, welcher Betrag höher ist) betragen.

Die nachfolgenden Hinweise beruhen auf der Bekanntmachung „Datenschutz-Check 2018: Was müssen Arztpraxen angesichts der neuen Vorschriften zum Datenschutz tun?“ der Bundesärztekammer/Kassenärztliche Bundesvereinigung (Bekanntmachung im DÄ /Jg.115/Heft 10/ 9. März 2018) und den „Hinweisen und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer/Kassenärztliche Bundesvereinigung (Bekanntmachung im DÄ /Jg.115/Heft 10/ 9. März 2018 – Online DOI: 10.3238/arztebl.2018.ds01). Hinzufügungen zum o. g. Datenschutz-Check 2018 sind durch Kursivschrift kenntlich gemacht.

I. Interne Datenschutzorganisation/Datenschutzmanagement in der Arztpraxis

Ärztinnen und Ärzte benötigen für Ihre Praxis ein Datenschutzmanagement, um sicherzustellen und dokumentiert nachweisen zu können, dass sie den Datenschutz entsprechend der EU-DSGVO wahren. Das umfasst unter anderem:

1. Benennung eines Datenschutzbeauftragten

Einige Arztpraxen werden einen Datenschutzbeauftragten zu benennen haben (Art. 37 EU-DSGVO), der entweder in der Praxis beschäftigt ist oder als externer Dienstleister beauftragt wird. Das ist in jedem Fall anzunehmen, wenn Ärzte in der Praxis mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 BDSG neu).

Unabhängig davon kann eine Pflicht zur Benennung eines Datenschutzbeauftragten bestehen, wenn ein hohes Risiko für die Rechte und Freiheiten der Patienten durch die Datenverarbeitung (z. B. bei der Verarbeitung genetischer Daten) besteht oder eine umfangreiche Verarbeitung von Gesundheitsdaten (z. B. durch eine große Anzahl von Patientendatensätzen) erfolgt. Letzteres ist für Einzelarztpraxen und Praxisgemeinschaften i. d. R. auszuschließen. In vielen Gemeinschaftspraxen findet im Vergleich zum durchschnittlichen Einzelarzt aber keine umfangreiche Verarbeitung statt, so dass auch hier kein Datenschützer erforderlich ist. Hier ist hier leider noch vieles unklar. Wir werden so bald wie möglich hierzu konkretere Hinweise nachliefern.

Die zu benennende Person, die nicht der Praxisinhaber sein kann, muss für diese Aufgabe fachlich qualifiziert sein. Die notwendigen Fachkenntnisse können z. B. über Schulungen erworben werden. Der Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde zu melden *und seine Kontaktdaten sind zu veröffentlichen*. Er kontrolliert intern nicht nur die Einhaltung des Datenschutzes und der Datensicherheit, z. B. durch geeignete technisch-organisatorische Maßnahmen, sondern er dient auch als kompetenter Ansprechpartner für alle im Zusammenhang mit dem Datenschutz aufkommenden Fragen.

Es kann auch ein externer Datenschützer benannt werden.

2. Erstellung eines Verzeichnisses für Verarbeitungsvorgänge in der Arztpraxis

Es ist eine Bestandsaufnahme erforderlich, welche Daten in der Arztpraxis auf welcher Rechtsgrundlage verarbeitet werden. Alle Arztpraxen haben ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Art. 30 EU-DSGVO), wobei für jede Gruppe von Datenverarbeitungsvorgängen ein entsprechendes Formular auszufüllen ist. Es sind verschiedene Muster im Internet abrufbar (siehe die Übersicht unter V.)

3. Überprüfung aller internen Verarbeitungsvorgänge in der Arztpraxis

Alle elektronischen Verarbeitungsvorgänge sowie die Verarbeitung von Patientendaten in Karteien sind auf die datenschutzrechtliche Konformität hin zu überprüfen. Insbesondere müssen geeignete technisch-organisatorische Maßnahmen ergriffen werden *(siehe DÄBl. 19/2008, S. 1 ff und DÄBl. 21/2014, A-969 ff)*. Unter Umständen muss auch eine sog. Datenschutzfolgenabschätzung durchgeführt werden (Art. 35 EU-DSGVO), um voraussichtliche Risiken bei der Verarbeitung von Patientendaten abzuschätzen und Maßnahmen der Abhilfe zu bestimmen*. Das ist wie bei der Pflicht zur Benennung eines Datenschutzbeauftragten dann der Fall, wenn ein hohes Risiko für die Rechte und Freiheiten der Patienten durch die Datenverarbeitung besteht oder eine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt*. Ansprechpartner hierfür ist ggf. der Landesbeauftragte für den Datenschutz.

4. Sicherheit der Datenverarbeitung

Durch geeignete technisch-organisatorische Maßnahmen (z. B. beschränkte Zugriffsrechte der Mitarbeiter oder Verschlüsselungsmaßnahmen, siehe DÄBl. 19/2008, S. 1 ff und DÄBl. 21/2014, A-969 ff) ist die Sicherheit der Datenverarbeitung in der Arztpraxis, insbesondere vor Angreifern von außen, zu gewährleisten.

5. Erarbeitung einer internen Datenschutzrichtlinie

Um in Arztpraxen ein Bewusstsein für den Datenschutz und Datenschutzrisiken zu schaffen, kann die Erstellung einer internen Datenschutzrichtlinie sinnvoll sein, in der z. B. Verhaltensweisen bei Erfassung von Patientendaten, klare Verantwortlichkeiten oder Zugriffsbeschränkungen für Mitarbeiter festgelegt werden können. Bestimmt werden kann darin auch, wie und wo der Nachweis über die einschlägige Rechtgrundlage der Verarbeitung (z. B. eine gesetzliche Bestimmung oder eine Einwilligung) dokumentiert werden kann.

6. Überprüfung und Anpassung vorhandener Verträge und Formulare

Sowohl Einwilligungserklärungen als auch verwendete Verträge mit Dritten, welche Datenverarbeitungsvorgänge betreffen, sind möglicherweise an das neue Datenschutzrecht anzupassen (siehe unter II. und III.).

II. Verhältnis zum Patienten

1. Einholung von Einwilligungserklärungen für besondere Datenverarbeitungsvorgänge

Im Rahmen der routinemäßigen Behandlung von Patienten beruht die Datenverarbeitung meist auf einer gesetzlichen Grundlage, sodass eine Einwilligung zur Datenverarbeitung in der Regel nicht einzuholen ist. *Bei der Teilnahme an Selektivverträgen ist zwar nach den Regeln des SGB V eine datenschutzrechtliche (nicht im Sinne der ärztlichen Schweigepflicht nach dem Strafgesetzbuch, hier ist die Weiterleitung der Daten an die Abrechnungsstellen durch § 295a SGB V legitimiert!) Einwilligung gefordert. Diese Patienteneinwilligung war aber bisher in Baden-Württemberg bereits Vertragsbestandteil und wird derzeit von den Vertragspartnern angepasst.* Soweit ausnahmsweise Einwilligungserklärungen für bestimmte Datenverarbeitungsvorgänge (z. B. Einbeziehung einer privaten Verrechnungsstelle) erforderlich sind und noch nicht eingeholt worden sind,

ist dieses nachzuholen. *Grundsätze für eine Einwilligung sind: Informiertheit, Bestimmtheit und Verbot der Pauschaleinwilligung (der Patient muss erkennen können, zu welchem Verarbeitungszweck er die Einwilligung erteilt, welche Daten in welchem Umfang verarbeitet werden sollen und welchen Personen er die Verarbeitung seiner Gesundheitsdaten gestatten soll), Ausdrücklichkeit und Freiwilligkeit. Einwilligungserklärungen müssen auch den Hinweis auf die Widerrufbarkeit enthalten.*

Das Vorliegen von Einwilligungserklärungen zur Datenverarbeitung muss durch den Praxisinhaber nachgewiesen werden.

2. Informationspflichten

Mit Blick auf die ausgeweiteten Informationspflichten (Art. 12-14 EU-DSGVO) können entsprechende Vordrucke genutzt werden, über die Patienten in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache informiert werden. Denkbar ist, dass diese z. B. sichtbar in der Arztpraxis ausgehängt werden. Entsprechende Vordrucke werden erarbeitet, *siehe unter V.*

3. Auskunftsrecht des Patienten

Neben dem Einsichtsrecht gemäß § 630g BGB (Behandlungsvertrag) existiert das datenschutzrechtliche Auskunftsrecht (Art. 15 EU-DSGVO), wonach Patienten vom Arzt Auskunft über die zu ihrer Person ggf. gespeicherten Daten verlangen können. Dafür sollte in einer internen Datenschutzrichtlinie ein bestimmtes Verfahren eingerichtet werden, um entsprechende Anfragen schnell beantworten zu können. Es ist zu beachten, dass kein Anspruch des Patienten besteht, Auskunft über personenbezogene Daten anderer Betroffener (Dritter) zu erhalten.

Achtung: *Das in Art. 20 der EU-DSGVO vorgesehene Recht des Patienten auf kostenlosen Erhalt ihrer Daten in strukturierter, gängiger und maschinenlesbarer Form betrifft nur Daten, die von den Patienten auf Basis einer Einwilligung selbst zur Verfügung gestellt wurden (z. B. aus Fitness-Apps)!*

4. Recht auf Löschung

Im Zusammenhang mit den Aufbewahrungsfristen sind Löschungsfristen (Art. 17 EU-DSGVO) zu berücksichtigen. Dafür sollte in einer internen Datenschutzrichtlinie ein bestimmtes Verfahren festgelegt werden, z. B. wann und durch wen die Daten z. B. nach Ablauf von Aufbewahrungsfristen gelöscht werden sollen.

Ein Anspruch der Patienten auf unverzügliche Löschung ihrer Daten besteht insbesondere, wenn diese Patientendaten nicht mehr benötigt werden, die Einwilligung in die Verarbeitung widerrufen wurde, ein Widerspruch gegen die Verarbeitung erklärt wurde oder die Speicherung unzulässig ist. Ein Anspruch des Patienten auf Löschung kommt aber nicht in Betracht, wenn dem eine vertragliche oder satzungsgemäße Aufbewahrungspflicht entgegensteht. Für den Bereich der ärztlichen Dokumentation gilt grundsätzlich eine zehnjährige Aufbewahrungspflicht; in diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung.

III. Verhältnis zu externen Dienstleistern und Dritten

Soweit Verträge mit externen Dienstleistern, z. B. zur Ausführung von Wartungsaufgaben an der Praxis-EDV-Anlage oder mit Privaten Verrechnungsstellen, bestehen oder abgeschlossen werden sollen, müssen diese Verträge auf ihre Vereinbarkeit mit den neuen datenschutzrechtlichen Vorschriften sowie mit den strafrechtlichen Bestimmungen zur ärztlichen Schweigepflicht überprüft werden.

1. Anpassung vertraglicher Vereinbarung mit externen Dienstleistern nach den Vorschriften zur Auftragsverarbeitung

Sofern es sich um eine Auftragsverarbeitung handelt (z. B. Wartungsdienste für die Praxis-EDV oder Nutzung von Cloud-Diensten), sollten entsprechende Vereinbarungen getroffen werden, deren Anforderungen sich aus Art. 28 Abs. 3 EU-DSGVO ergeben. Es existieren Muster im Internet, *siehe unter V*.

2. Verpflichtung zur Geheimhaltung

In Verträgen mit externen Dienstleistern sind neben den datenschutzrechtlichen Vorgaben auch Verpflichtungen aufzunehmen, nach denen die mitwirkenden Dritten zur Geheimhaltung verpflichtet werden. Das Unterlassen kann zu einer Strafbarkeit führen!

IV. Verhältnis zu Aufsichtsbehörden für den Datenschutz und anderen Stellen

1. Befugnisse der Aufsichtsbehörden für den Datenschutz

Es ist zu beachten, dass Aufsichtsbehörden nur eingeschränkte Rechte gegenüber Berufsgeheimnisträgern haben, insbesondere erfolgt keine umfassende Auskunft über Patientengeheimnisse an die Aufsichtsbehörden. Für die Aufsichtsbehörden bestehen nur beschränkte Durchsuchungs- und Betretungsrechte in der Arztpraxis, soweit ihre Maßnahmen einen Verstoß gegen die Geheimhaltungspflichten von Ärzten zur Folge hätten. Von einer generellen Verweigerung unter Berufung auf die ärztliche Schweigepflicht ist abzuraten, da eine unberechtigte Verweigerung ein Bußgeld nach sich ziehen kann.

2. Keine Pflicht zur umfassenden Auskunft bei Selbstbelastung

Wie bisher kann die Auskunft auf Fragen verweigert werden, deren Beantwortung die Gefahr einer strafgerichtlichen Verfolgung (z. B. wegen des Verstoßes gegen die ärztliche Schweigepflicht) nach sich ziehen würde. Es besteht grundsätzlich keine Pflicht, sich selbst zu belasten!

3. Meldung von Datenpannen und –verstößen

Datenpannen (z. B. Hackerangriffe) und Datenschutzverstöße (z. B. durch Mitarbeiter) sind in der Regel der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden zu melden. Dafür sollte in einer internen Datenschutzrichtlinie festgelegt werden, wer für die Meldung zuständig ist. Die Meldepflicht ist problematisch, sofern der Verantwortliche sich selbst belasten würde, einen Verstoß gegen die ärztliche Schweigepflicht begangen zu haben. Die Meldung ist dann zwar vorzunehmen. Es besteht aber ein prozessuales Verwertungsverbot und die Meldung kann in einem Strafverfahren oder im Ordnungswidrigkeitenverfahren nur mit Zustimmung des Arztes verwendet werden.

4. Schulungsangebote der Aufsichtsbehörden und Ärztekammern in Anspruch nehmen

Soweit im jeweiligen Bundesland verfügbar, können Schulungsangebote in Anspruch genommen werden (z. B. der Landesbeauftragten für den Datenschutz, Kassenärztlichen Vereinigungen oder der Ärztekammern), um eine Vorbereitung auf die neue Rechtslage sicherzustellen.

V. Weitere Hinweise und Muster

1. Weiterführende Hinweise

Weitere Hinweise zum Datenschutz sowie zu Neuregelungen im Bereich der ärztlichen Schweigepflicht erhalten Sie in *Bundesärztekammer/Kassenärztliche Bundesvereinigung*:
„Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis.

Die Europäische Kommission informiert hier: https://ec.europa.eu/commission/priorities/justiceand-fundamental-rights/data-protection/2018-reform-eu-data-protectionrules_de#berdieverordnungunddatenschutz s.a. hier: https://ec.europa.eu/info/law/law-topic/dataprotection/reform/rules-business-and-organisations_de

Die Aufsichtsbehörden für den Datenschutz erstellen sukzessive Kurzpapiere zu den wichtigsten datenschutzrechtlichen Themen. Sie sind hier abrufbar:
https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Einen 10-Punkte-Fragenkatalog für Unternehmen stellt u. a. die Landesbeauftrage für den Datenschutz in Niedersachsen zur Verfügung, abrufbar unter:
https://www.lfd.niedersachsen.de/download/124239

KBV-Internetseite: **http://www.kbv.de/html/datensicherheit.php**

Einen Fragebogen für Arztpraxen gibt es beim Landesbeauftrage für den Datenschutz in Mecklenburg-Vorpommern unter
https://www.datenschutz-mv.de/static/DS/Dateien/.../Fragebogenaktion/Fragebogen.pd...

Darüber hinaus sind regelmäßig aktualisierte Informationen auf den Internetseiten der Aufsichtsbehörden (Landesbeauftragte für Datenschutz und Informationsfreiheit) verfügbar. Eine Übersicht der Aufsichtsbehörden für den Datenschutz und der Landesdatenschutzbeauftragten findet sich hier:
https://www.datenschutzwiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

2. Muster

Ferner finden sich Muster im Internet, die aber teilweise noch nicht mit den Aufsichtsbehörden abgestimmt sind. Für die Richtigkeit der Muster wird von uns keine Gewähr übernommen.

Muster für ein Verzeichnis der Verarbeitungstätigkeiten

Siehe zurzeit das vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. zur Verfügung gestellte Muster, abrufbar unter:
https://www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/
oder
https://www.bvdnet.de/wpcontent/uploads/2017/06/Muster_Verz_der_Verarbeitungst%C3%A4tigkeiten_Verantwortlicher.pdf

Siehe auch das von der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. erstellte Muster, abrufbar unter: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

Siehe auch die Hinweise zum Verzeichnis der Verarbeitungstätigkeiten der Datenschutzkonferenz, abrufbar unter:
https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutzgrundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/

Muster für Auftragsverarbeitungsverträge

Siehe z. B. das vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., der DKG u. a. ausgearbeitete „Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen“, abrufbar hier: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

Siehe auch die Formulierungshilfe für einen Auftragsverarbeitungsvertrag des Bayrischen Landesamtes für Datenschutzaufsicht, abrufbar unter: https://datenschutz.sachsenanhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/auftrags_dv/Muster_fuer_Auftragsverarbeitungsvertrag_nach_DS-GVO.pdf

Muster zur Umsetzung von Informationspflichten

Siehe zurzeit das von der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. erstellte Muster „GDD-Praxishilfe DS-GVO VII“, S. 8 ff., abrufbar unter:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf