DEUTSCHER HAUSÄRZTEVERBAND

Das neue Datenschutzrecht – *MERKBLATT* für Hausärzte* mit *Mustertexten und Checklisten* – Stand 25.05.2018

I. Hintergrund, Wichtigkeit des Themas

Am 25. Mai 2018 tritt ein neues Datenschutzrecht in Kraft: Das bisherige Bundesdatenschutzgesetz wird durch die DS-GVO (Datenschutz-Grundverordnung) ersetzt. In der Arztpraxis besteht Handlungsbedarf, da sich datenschutzrechtliche Pflichten ändern, und bei Nichtbefolgung der Anforderungen hohe Bußgelder drohen.

CAVE: Weitere allgemeine und beachtenswerte Informationen

- BÄK/KBV, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt v. 9. März 2018
- BÄK/KBV, Datenschutz-Check 2018: Was müssen Arztpraxen angesichts der neuen Vorschriften zum Datenschutz tun?, Deutsches Ärzteblatt v. 9. März 2018
- KBV, Datenschutz Grundverordnung März 2018 Ab 25. Mai gelten neue Vorschriften beim Datenschutz: Was Praxen jetzt tun müssen, http://www.kbv.de/media/sp/Praxisinformation_Datenschutz_DSGVO.pdf
- ULD Schleswig – Holstein, https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html

II. Allgemeine Hinweise (vgl. Muster „Merkblatt für Patienten“)

Datenschutzrecht betrifft den Schutz von **personenbezogenen Daten**. Das sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer Person, insbesondere also Patienten und Mitarbeiter. Beispiele sind Name und Anschrift, Geburtsdatum, Bankverbindung u. ä. Die Art der Erfassung (digital oder auf Papier) spielt keine Rolle. Der Datenschutz bezieht sich auf jede Form des **Verarbeitens**, also z. B. Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen.

Nach der DS-GVO sind Verarbeitungen grundsätzlich verboten, es sei denn, es besteht eine Erlaubnis im Gesetz. In der Praxis werden Datenverarbeitungen vielfach durch deren Notwendigkeit für die **Erfüllung vertraglicher Pflichten** (z. B. Behandlungsvertrag, Arbeitsvertrag) gerechtfertigt sein. Schließlich kann eine **informierte und freiwillige Einwilligung** eingeholt werden.

In jedem Fall muss allerdings über die Datenverarbeitung informiert werden, Art. 13 DS-GVO.

Die DS-GVO enthält eine Reihe weiterer relevanter Regelungen, wie z. B. die Pflicht zur Erstellung eines Verfahrensverzeichnisses, Pflichten zur IT-Sicherheit, Benachrichtigungspflichten bei

Datenpannen, Auskunftsrechte der betroffenen Personen. Bei besonderen datenschutzrechtlichen Gefahrenlagen ist eine sog. Datenschutz-Folgenabschätzung durchzuführen.

CAVE: Weitere allgemeine Informationen mit Mustertexten

- Bayerisches Landesamt für Datenschutzaufsicht, Anforderungen der DS-GVO an kleine Unternehmen, Vereine, etc. – Muster 5: Arztpraxis
- BITKOM, FAQ: Was muss ich wissen zur Datenschutz-Grundverordnung?

III. Konkrete nächste Schritte

Die folgenden Maßnahmen und Schritte sind das absolute Minimum im Hinblick auf die datenschutzrechtlichen Verpflichtungen des niedergelassenen Hausarztes. Sie ersetzen nicht eine umfassendere Befassung mit dem Thema Datenschutz. Zusätzliche Verarbeitungen, wie z. B. der Einsatz von Videoüberwachung, erfordern zusätzliche Klärungen und Dokumentation.

1. Verzeichnis von Verarbeitungstätigkeiten (vgl. Muster „Verarbeitungsverzeichnis“)

Art. 30 DS-GVO verpflichtet dazu, ein sog. Verzeichnis von Verarbeitungstätigkeiten zu führen. Hier sind die wesentlichen Verarbeitungstätigkeiten, die verarbeiteten Daten, die Zwecke der Verarbeitung und die Rechtsgrundlage zu dokumentieren.

CAVE: Weitere allgemeine Informationen und Mustertexte

- Bayerisches Landesamt für Datenschutzaufsicht, Muster 5: Arztpraxis – Verzeichnis von Verarbeitungstätigkeiten
- KBV, Muster für Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzkonferenz, Kurzpapier 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
- Datenschutzkonferenz, Muster für Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Word-Version)

2. Überprüfung/Aktualisierung der IT-Sicherheit, Datenpannen, Löschkonzept (vgl. „Checkliste TOM“)

Die DS-GVO erhöht die Anforderungen an die IT-Sicherheit. Hinzu kommen Informationspflichten bei Datenpannen. Zu den notwendigen Maßnahmen gehört insbesondere die regelmäßige Aktualisierung der eingesetzten Hard- und Software; insb. durch das Einspielen von Fehlerbeseitigungen. Soweit keine Rechtsgrundlage mehr für die Speicherung von personenbezogenen Daten besteht (gesetzliche Aufbewahrungsfristen, Verjährung möglicher Haftungsansprüche), sind diese zu löschen.

CAVE: Weitere allgemeine Informationen, Muster und Checklisten

- Die Landesbeauftragte für den Datenschutz Nordrhein- Westfalen, Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand
- KVN, Selbst-Check: Datenschutz in der Arztpraxis
- KBV, Aufstellung der Maßnahmen zum Datenschutz
- Bundesärztekammer, Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis (wird derzeit überarbeitet)
- Bayerisches Landesamt für Datenschutzaufsicht, Umgang mit Datenpannen

3. Datenschutzbeauftragter (vgl. Muster „Benennung eines Mitarbeiters zum DSB“ und „Benennung eines ehrenamtlichen DSB“)

Häufig wird es nicht erforderlich sein, einen Datenschutzbeauftragten zu ernennen, sofern weniger als zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (**merke**: „ständig beschäftigt“ ist die Medizinische Fachangestellte; „nicht ständig beschäftigt“ ist die Reinigungsfachkraft, die theoretisch personenbezogene Daten zur Kenntnis nehmen kann). Dies gilt allerdings nur dann, wenn keine überdurchschnittlichen Umfänge oder Intensitäten der Datenverarbeitung erreicht werden.

CAVE: **Weitere allgemeine Informationen**

- DSK, Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
- BÄK/KBV, Kapitel 3.9 der Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt v. 9. März 2018
- Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018 - Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Datenschutz/DSK/Entschliessungen/095_DSB-Bestellpflicht.pdf

4. Datenschutz-Verpflichtung von Beschäftigten (vgl. Muster „Verpflichtung Einhaltung Anforderungen MFA und VERAH“ und Muster „Verzeichnis von Verarbeitungstätigkeit – Ausfüllhilfe“)

Bei der Aufnahme der Beschäftigung sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt. Hinzu kommt wie bisher die Verpflichtung, Angestellte weiterhin auch nach § 203 StGB zu belehren. Die Belehrungen sollten schriftlich dokumentiert werden.

CAVE: **Weitere allgemeine Informationenmit Muster für eine Belehrung**

- Bayerisches Landesamt für Datenschutzaufsicht, Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

5. Auftragsverarbeitung

Sofern Externe in Anspruch genommen werden, um personenbezogene Daten verarbeiten zu lassen, ist ein Vertrag zur Auftragsdatenverarbeitung erforderlich. Die bisherige Regelung in § 11 BDSG wurde in Art. 28 DS-GVO überführt und erweitert. **Bestehende Verträge müssen überprüft und ggf. angepasst werden.**

Hinzu kommt die Änderung von § 203 StGB im vergangenen Jahr: Externe müssen jetzt nach § 203 StGB belehrt werden, wenn eine Strafbarkeit nach § 203 StGB vermieden werden soll. Die Belehrungen sollten schriftlich dokumentiert werden.

Die großen IT-Dienstleister, die HÄVG Rechenzentrum GmbH und auch die HÄVG Hausärztliche Vertragsgemeinschaft AG haben die notwendigen Aktualisierungen ihrer Dokumentation vorgenommen und stellen diese rechtzeitig zur Verfügung. Weitere Informationen erhalten die an der Hausarztzentrierten Versorgung (HZV) teilnehmenden Hausärzte von dort aus.

CAVE: Weitere allgemeine Informationen mit Formulierungshilfen

- Bayerisches Landesamt für Datenschutzaufsicht, Formulierungshilfe für einen Vertrag zur Auftragsverarbeitung
- Datenschutzkonferenz, Kurzpapier Nr. 13 – Auftragsverarbeitung, Artikel 28 DS-GVO
- KBV - Datenschutz Grundverordnung März 2018 http://www.kbv.de/media/sp/Praxisinformation_Datenschutz_DSGVO.pdf

6. Informations- und Auskunftspflichten

Schon bei der Datenerhebung müssen den betroffenen Personen bestimmte Informationen zur Verfügung gestellt werden. Mindestens muss darauf hingewiesen werden, wo die Informationen leicht zugänglich sind (z. B. Flyer, Aushang, Homepage). Eine Möglichkeit für die entsprechende Information kann sein, ein (gekürztes) Verarbeitungsverzeichnis im Wartezimmer auszulegen. Insoweit aktualisierte Info-Texte für die HZV werden direkt von der HÄVG AG zur Verfügung gestellt.

Darüber hinaus haben die betroffenen Personen das Recht, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten.

CAVE: Weitere allgemeine Informationen und Muster

- KBV, Muster für Patienteninformation
- Datenschutzkonferenz, Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung

6.1 Datenschutzhinweise auf Internetseiten oder in Social Media-Portalen (Facebook, XING, Twitter, etc.,)

Vielfach nutzen Hausarztpraxen eigene Internet- und/oder sog. Social Media-Seiten zur Präsentation ihrer Praxis und ihrer Angebote/Services

Solche Seiten müssen eine Datenschutzerklärung mit folgenden **Mindestangaben** beinhalten:

Hinweise darauf, dass

- personenbezogene Daten wie Name, Postanschrift, E-Mail-Adresse, Telefonnummer oder das Geburtsdatum ausschließlich in Übereinstimmung mit dem jeweils geltenden Datenschutzrecht erhoben und genutzt werden
- Daten nur gespeichert werden, wenn sie aktiv übermittelt werden
- Daten zum Beispiel nur zur Beantwortung von Anfragen oder zur Zusendung von Informationsmaterial verwendet werden
- Kontaktdaten, die im Rahmen von Anfragen angegeben werden, ausschließlich für die Korrespondenz verwendet werden

- E-Mail-Adressen, die Nutzer für den Bezug eines Newsletters angegeben haben, nur dafür genutzt werden

Es bietet sich zudem an, dass **Merkblatt für Patienten** zum Datenschutz auf der Internetseite der Praxis einzustellen. Ferner empfiehlt es sich die inhaltliche Ausgestaltung der Datenschutzerklärung mit dem jeweiligen Provider bzw. IT – Beauftragten abzustimmen.

Allgemeine Muster für Datenschutzerklärungen finden sich zum Beispiel unter:

https://www.datenschutz.org/datenschutzerklaerung-website/#datenschutzerklaerung-fuer-eine-website-vorlage-zum-download

7. Einwilligungserklärungen aktualisieren

Sofern Einwilligungserklärungen verwendet werden, sollten diese durchgesehen und aktualisiert werden. Insbesondere das Thema Freiwilligkeit der Einwilligung und der Hinweis auf das Widerspruchsrecht der Patienten bedürfen einer stärkeren Hervorhebung.

CAVE: Weitere allgemeine und spezifische Informationen

- Bayerisches Landesamt für Datenschutzaufsicht, Einwilligungen nach der DS-GVO
- BÄK/KBV, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt v. 9. März 2018 (unter 2.4.1)

ANLAGEN: MUSTER / CHECKLISTE

* Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige beider Geschlechter.