Datenschutz-Grundverordnung und Bundesdatenschutzgesetz

Anwendungsbereiche in der Arztpraxis - eine Zusammenfassung

ARBEITSGEMEINSCHAFT BERLINER ARZTNETZE

Referent

- Herr Albrecht Römpp, M.A.
  Arbeitsgemeinschaft Berliner Arztnetze GmbH & Co.KG, www.agban.de
  - Trainer und Berater im Gesundheitswesen
  - seit 2005 zu Themen wie Datenschutz, QM, Praxisorganisation deutschlandweit über 500 Seminare und Beratungen
  - Netzmanager von 3 Arztnetzen in Berlin
  - Kontakt: datenschutzbeauftragter@agban.de

ARBEITSGEMEINSCHAFT BERLINER ARZTNETZE

Hinweis

1. Bislang sind viele Punkte der DSGVO noch nicht abschließend rechtlich geklärt. Wir können daher zu einigen Fragen nur Empfehlungen aussprechen
2. Mit wenigen Ausnahmen sind die nachfolgenden Anforderungen zum Datenschutz in der Arztpraxis nicht neu und auch schon aktuell im Bundesdatenschutzgesetzt alter Fassung gefordert.
3. Für Praxen, welche bisher schon einen hohen Datenschutzstandard umgesetzt haben, ändert sich daher nicht viel!

DS-GVO

- Veröffentlichung im EU-Amtsblatt am 04. Mai 2016. Stichtag für die Umsetzung ist somit der **25.05.2018**.
- Bis zu diesem Zeitpunkt müssen alle Dokumente und Prozesse der Datenverarbeitung an die neue Regelung angepasst sein.
- Das an die europäische Richtlinie angepasste BDSG n.F. (neue Fassung) tritt ebenfalls am 25.05.2018 in Kraft.

Das ist in der Praxis wichtig!

- **Einverständniserklärung** zur Datenweitergabe
- **Aushang** „Information der Patienten zur Datenverarbeitung in der Praxis“
- **Schriftliche** Bestellung eines Datenschutzbeauftragten
- **Verzeichnis** zu (Daten-) Verarbeitungstätigkeiten
- **Verträge** zur Auftragsverarbeitung mit externen Dienstleistern (Datenverarbeitung im Auftrag)
- **Datenschutzerklärung** für Homepage
- **Interne Regelungen** zum Datenschutz und zur Diskretion, Unterweisung der Mitarbeiter (im Rahmen Ihres QM!)

Gesetzlicher Rahmen im Datenschutz

- § 203 Strafgesetzbuch (StGB)
- § 9 Berufsordnung der Ärzte (MBO-Ä)
- Europäische Datenschutz-Grundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG n.F.)
- §§ 630a ff. Bürgerliches Gesetzbuch (BGB)
- Sozialgesetzbuch V (SGB V)

Ärztliche Schweigepflicht (§203 StGB)

- Adressaten:
  - Arzt und Angehörige eines anderen Heilberufes
  - berufsmäßig tätige Gehilfen (z.B. med. Fachangestellte)
- Reichweite:
  - auch gegenüber anderen Ärzten und Familienangehörigen
  - auch gegenüber Minderjährigen
  - auch nach dem Tod des Patienten
- Offenbarungsbefugnisse:
  - Einwilligung des Betroffenen (schriftlich)
  - Gesetzliche Mitteilungspflichten oder -erlaubnisse (z.B. SGB V)
  - Rechtfertiger Notstand gem. § 34 StGB
  - Gesetzes zur Kooperation und Information im Kinderschutz (KKG)

Offenbarung

- Nur zulässig, wenn sie entweder durch eine gesetzliche Vorschrift, durch Einwilligung des Patienten oder einen besonderen Rechtfertigungsgrund legitimiert ist
  - Mündliche Einwilligung („ich rufe da mal kurz an“)
  - Konkludente Einwilligung (z.B. Dolmetscher, Notfall)
  - Schriftliche Einwilligung (z.B. nach §73b, PVS)
- Die schriftliche Einwilligung ist insbes. immer dann empfohlen, wenn keine gesetzliche Verpflichtung zur Weitergabe von personenbezogenen Daten an Dritte vorliegt

Information der Patienten

- Art 13 DS-GVO i. V. m. §32ff BDSG
- Information zur Art und Umfang der Datenverarbeitung (was, warum, an wen?)
- Wer ist verantwortlich für die Datenverarbeitung, Kontakt des Datenschutzbeauftragten?
- Rechtsgrundlage der Datenverarbeitung
- (gesetzliche) Speicherfristen
- Recht auf Widerruf, Recht auf Einsichtnahme, Hinweis auf Beschwerdemöglichkeiten
- Übermittlung in Drittstaaten, Profiling

Information der Patienten

Art. 12 DSGVO:

- präzise,
- transparent,
- verständlich
- und in leicht zugänglicher Form
- in einer klaren und einfachen Sprache
- in Papierform oder elektronisch

Z.B.: Homepage, Aushang in der Praxis, Handzettel zur Abgabe z.B. bei schriftlichem Einverständnis zur Datenweitergabe

Einsichtnahme

- **§ 639g BGB:** „Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen“
- **Art 15ff DS-GVO:** Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten (…)

Recht auf Vergessen

- Art. 17 DS-GVO
- Löschen von Daten bei
  - Wiederruf einer Einwilligung
  - Unrechtmäßig erhobenen Daten
  - Fehlender Notwendigkeit/kein berechtigtes Interesse
  - Recht auf Berichtigung

Ausnahmen:

- Es steht dem ein Rechtsgrund wie z.B. Aufbewahrungspflichten oder das Beweissicherungsinteresse (s. KVNO aktuell 3+4, 2015) entgegen
- Das Geltend machen von Rechtsansprüchen, z.B. Honoraransprüche

Betrieblicher Datenschutzbeauftragter

Erforderlich, wenn

- gemäß Artikeln 37 ff. DS-GVO die Kerntätigkeit des Verantwortlichen in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** (z.B. Gesundheitsdaten, Art. 9 DS-GVO) liegt
- Ergänzend gemäß § 38 Bundesdatenschutzgesetz n.F., soweit in der Regel **mindestens 10 Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden.
- Gemäß Art. 35 DS-GVO die Notwendigkeit einer **Datenschutz-Folgenabschätzung** vorliegt

Betrieblicher Datenschutzbeauftragter

Unabhängig davon, ob eine Bestellpflicht besteht oder nicht:

- die Benennung einer verantwortlichen Person für den Datenschutz in Ihrer Praxis ist dringend empfohlen, da es sich bei Gesundheitsdaten um **besonderer Kategorien von Daten** (Art. 9 DS-GVO) handelt und eine besondere Sorgfaltspflicht nachgewiesen werden muss.

Bestellung des bDSB

- Inhaber darf nicht als bDSB bestellt werden!
- Schriftlich, als Vertrag oder Ernennungsschreiben, darin enthalten sind Rechte und Pflichten
- spätestens einen Monat nach Aufnahme einer bestellpflichtigen Tätigkeit
- Pflichten: Überwachung der Einhaltung aller Datenschutzvorschriften, Beratung, Information und Schulung aller Beteiligten/der Leitung
- Kann intern oder extern bestellt werden, sollte fachlich geeignet und zuverlässig sein
- Meldung an die Aufsichtsbehörden (nach dem 25.5.2018), Aushang in der Praxis, Homepage
- Hat einen starken Kündigungsschutz (Unabhängigkeit)

Verarbeitungsverzeichnis (Art. 30 DS-GVO)

- Verzeichnis (schriftlich oder elektronisch) aller Kategorien von Verarbeitungstätigkeiten mit folgenden Angaben:
  - Namen und Kontaktdaten des Verantwortlichen, der bDSB
  - die Zwecke der Verarbeitung, Empfänger von Daten
  - betroffene Personen und Kategorien personenbezogener Daten, (Rechtsgrundlage der Verarbeitung)
  - Fristen für die Löschung, Überprüfung der Erforderlichkeit der Speicherung
  - allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
- Ist auf Anforderung den Behörde zur Verfügung zu stellen

Verarbeitungsverzeichnis

In einer "normalen" Arztpraxis dürften das vor allem folgende Verarbeitungstätigkeiten sein:

- Dokumentation der Behandlung im AIS
- Abrechnung KV, Privatleistung (PVS)
- Laboruntersuchungen (Labordatenübertragung)
- Wartungsverträge (z.B. AIS, EDV)
- Mitarbeiterdaten (Personalakten, Bewerbungsunterlagen, Lohnbuchhaltung)
- Kommunikation per E-Mail, Kontaktformular Website,
- Rezeptbestellung, Onlineterminsystem
- Lieferanten
- Weiter?

Auftragsverarbeitung (1)

Liegt gemäß § 62 Bundesdatenschutzgesetz n.F. vor, wenn personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet werden

- EDV-Betreuung (Fernwartung), Cloud-Dienst, Onlinetermine
- Datenträgerentsorgung
- Callcenter, (PVS)
- Externe Lohn- oder Gehaltsabrechnung
- Keine AV: Steuerberater oder Rechtsanwalt, Labor

Auftragsverarbeitung (2)

Wichtige Voraussetzung:

- Ist die unterstützende AV erforderlich?
- sogfältige Auswahl und Eignung des Auftragsnehmers
- Vertrag zur AV gemäß Anforderungen in § 62 BDSG, der die Einhaltung aller Datenschutzrechtlichen Bestimmungen sicherstellt (z.B. Verschwiegenheit, Löschen der Daten, TOM)
- Ggf. Kontrolle, der technischen und organisatorischen Maßnahmen des Auftragnehmers
- Gemeinsame Verantwortung im Haftungsfall, aber:

Gesamtverantwortung bleibt aber beim Auftragsgeber!!

IT-Sicherheit

Spielt eine große Rolle, insbes. dann, wenn über das Internet ein Zugriff auf das Praxisnetzwerk möglich ist

- Aktueller Stand der Sicherheitstechnik (Virenschutz, Firewall, Datenverschlüsselung, etc.),
- Elektronischer Versand ausschließlich mit gesicherten Verfahren (Verschlüsselung), Perspektivisch: Telematikinfrastruktur, E-Arztbrief
- Abschalten von nicht benötigten Schnittstellen (z.B. USB)
- fachgerechte Entsorgung von Festplatten und anderen Speichermedien, Aktenvernichter DIN 66399 Schutzklasse 3, Sicherheitsstufe 4

Technische und organisatorische Maßnahmen (TOM)

Art. 32 Abs 1, DS-GVO

z.B.

- Zugriffsschutz: abschließbare Schränke, Bildschirmschoner mit PW-Schutz, Benutzerrechte
- aktueller Virenscanner/Sicherheitssoftware (Firewall)
- Verschlüsselung beim elektronischen Versand, keine Speicherung in der Cloud bzw. außerhalb der EU (E-Mail, Apps, etc.),
- Interne Regelung Diskretion an der Anmeldung
- regelmäßige Schulungen/Unterweisungen der Mitarbeiter

Technische und organisatorische Maßnahmen (TOM)

- durch Tür abgetrennter Empfangs- und Wartebereich, schalldichte Türen
- Kein Zugriff für unbefugte auf mobile Geräte oder externe Speichermedien (PW-Schutz, Verschlüsselung)
- Erstellen eines Löschkonzepts
- regelmäßige Backups: z. B. täglich, wöchentlich auf einer externen Festplatte
- Notfallkonzept vorhanden: z. B. Regelung zum Verhalten bei Ausfall des AIS, Verhalten bei Virenbefall, Verhalten bei Verdacht auf Datenpannen (Hackerangriff)

Homepage

- Hinweis mit eine eigenen „Button“ auf datenschutzrechtliche Bestimmungen (Datenschutzerklärung)
- Umfang der Datenschutzerklärung hängt von der Art der Informationen und möglichen Interaktionen (z.B. Kontaktformular) der Homepage ab
- Angabe der Datenverarbeitung durch den **Provider** („statistische Zwecke“?!) mit aufnehmen!

Löschkonzept

- Das Löschkonzept muss die gesetzlichen Aufbewahrungsfristen berücksichtigen
- Bei Wiederruf einer Einwilligung müssen gespeicherte Daten gelöscht werden
- Dies gilt auch bei mangelndem berechtigtem Interesse oder bei unrechtmäßig erhobenen Daten
- **Ausnahmen**: Bei Erfüllung rechtlicher Verpflichtungen (z.B. Aufbewahrungsfristen) oder der Ausübung/Geltendmachung von Rechtsansprüchen (z.B. Privatrechnungen)

Datenschutz Folgenabschätzung

- gemäß § 70 Bundesdatenschutzgesetz n.F. in Verbindung mit Artikel 35 Datenschutz-Grundverordnung
- Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen
- Vorgeschaltet ist eine **Gefährdungsbeurteilung** (niedriges – mittleres-hohes Risiko nach Wahrscheinlichkeit des Gefährdungseintritts und Schweregrad der Gefährdung)
- Ist durchzuführen, wenn die Form der DV (insbes. bei neuen Technologien) aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich eine erhebliche Gefahr (**hohes Risiko**) für die Rechtsgüter (z.B. Recht auf informelle Selbstbestimmung) betroffener Personen zur Folge hat
- Einbeziehung der bDSB
- **Eine Liste aller Verarbeitungstätigkeiten, für die eine DSFA erforderlich ist, wird gerade von Bund und Ländern erarbeitet**

Datenpannen

- Zwingende Meldepflicht gegenüber Aufsichtsbehörden
  - Ausnahme: Die Datenpanne führt wahrscheinlich nicht zu einem Risiko für den Betroffenen
- Benachrichtigung des Betroffenen, wenn ein hohes Eingriffsrisiko besteht
- Eine Meldung sollte innerhalb von 72 Stunden erfolgen

Bußgeldrahmen (Art. 83 DS-GVO)

- Maximaler Bußgeldrahmen liegt bei 20.000.00 Euro oder 4 % des erzielten Jahresumsatzes
- Art, Schwere und Dauer des Verstoßes und Zusammenarbeit mit der Aufsichtsbehörde,
- Vorsatz oder Fahrlässigkeit, frühere Verstöße
- Getroffenen Maßnahmen zur Minderung des entstandenen Schadens
- Grad der Verantwortung des Verantwortlichen und getroffene technische und organisatorische Maßnahmen
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde (eigene Meldung, Anzeige durch Dritte)
- Jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste

Überwachung

- Wie und in welcher Form die Umsetzung der neuen Vorgaben nach dem 25.05.2018 überwacht werden ist (noch) nicht abzusehen
- Themen wie
  - Bestellung bDSB?
  - Verträge zur AV
  - „Betroffeneninformationen“
  - Verarbeitungsverzeichnis
  - Formular „Einwilligung Datenweitergabe“

sollten bis dahin aber nach Möglichkeit umgesetzt sein

Weiterführende Links

- KV Berlin: https://www.kvberlin.de/
  - Allgemeine Informationen
  - Musterdokumente
- KBV: http://www.kbv.de/html/datensicherheit.php
  - Checklisten, Allgemeine Informationen, Musterdokumente
- KV BaWü: https://www.kvbawue.de/praxis/unternehmen-praxis/datenschutz-schweigepflicht/
  - Musterdokumente
  - Auskunftspflichten „Um Antwort wird gebeten“

Unser Unterstützungsangebot

- „DS-GVO praktisch umsetzen“
  - Workshop für Mitarbeiter und Ärzte
  - Erstellen aller wichtigen Verzeichnisse und Datenschutzdokumente (TOM) unter fachlicher Anleitung,
  - Beantworten von Fragen
  - 3,5 h, kostet 119 inkl. Mwst.
  - In den Räumen der KV Berlin
  - Termine und Anmeldung über www.agban.de

ARBEITSGEMEINSCHAFT BERLINER ARZTNETZE

Noch Fragen?

Wir bedanken uns für Ihre Aufmerksamkeit und wünschen einen guten Nachhauseweg!

ARBEITSGEMEINSCHAFT BERLINER ARZTNETZE