Umsetzung der Datenschutzgrundverordnung in der Arztpraxis

I. Überblick

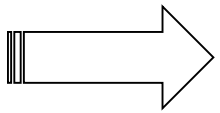
1. Grundsätzliches
2. Pflichten des Verantwortlichen (Art. 24-43)
3. Rechte des Betroffenen
4. Sanktionen

II. Aktuelle Fragestellungen

1. Datenschutzbeauftrager
2. Auskunftsrecht des Betroffenen
3. Recht auf Vergessenwerden

Auf einmal Datenschutz?

- **Beachtung von Datenschutzvorschriften in Arztpraxis schon immer**



- Mehr Transparenz
- Erweiterte Informationspflichten
- Strengere Sanktionen

➢ 1. Grundsätzliches

➢ personenbezogene Daten

- all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

➢ Verarbeiten (Art. 4 Ziff. 2 DSGVO)

- „*Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das* ***Erheben****, das* ***Erfassen****, die* ***Organisation****, das* ***Ordnen,*** *die* ***Speicherung****, die* ***Anpassung*** *oder* ***Veränderung****, das* ***Auslesen****, das* ***Abfragen****, die* ***Verwendung****, die* ***Offenlegung durch Übermittlung****,* ***Verbreitung*** *oder eine andere Form der* ***Bereitstellung****, den* ***Abgleich*** *oder die* ***Verknüpfung****, die* ***Einschränkung****, das* ***Löschen*** *oder die* ***Vernichtung****.*

- **Arztpraxis: besondere Kategorie von personenbezogenen Daten (Gesundheitsdaten)**

- **Art. 9 Abs. 1 DSGVO**

  „***Die Verarbeitung*** *personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,* ***Gesundheitsdaten*** *oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person* ***ist untersagt****.“*

Privilegierung der Gesundheitsberufe

- Verarbeitung ist im Rahmen des Gesundheitsberufes zur Durchführung des Gesundheitsberufes erlaubt.
- Gesetz Art. 9 Abs. 3 DSGVO
- Keine Einwilligungserklärung erforderlich, nur bei Datenweitergabe an Dritte
- Ärzte unterliegen – wie auch Anwälte – einem Berufsgeheimnis

➢ Verantwortlicher für Datenverarbeitung Art. 4 Ziff. 7 DSGVO

„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, ***die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet****; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;*

⇨ **Praxisinhaber ist Verantwortlicher**

➢ Rechtmäßigkeit der Verarbeitung Art. 6 DSGVO

- **Einwilligung** des Betroffenen (Art. 7 und Art 8 DSGVO)
- **Erfüllung eines Vertrages** oder vorvertraglicher Maßnahmen
- Erfüllung rechtlicher Verpflichtung
- Zur Wahrung berechtigter Interessen des Verantwortlichen/eines Dritten, wenn keine schutzwürdigen Interessen eines Betroffenen überwiegen

Häufig in Arztpraxis: - Erfüllung des **Behandlungsvertrag**
- **Einwilligung** bei Datenweitergabe an Dritte

2. Pflichten des Verantwortlichen

- Dokumentations- und Nachweispflichten (Verarbeitungsverzeichnis, Art. 30 DSGVO)
- Melde- und Benachrichtigungspflichten bei Datenpannen
- Technischer und organisatorischer Datenschutz
- Informationspflichten (Art. 12,13 DSGVO)

Hilfestellung gibt es z.B. von der Kassenärztlichen Bundesvereinigung

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

➢ Informationen mitteilen und zur Verfügung stellen

- Art. 13 Abs. 1 u. 2 DSGVO:

*Werden personenbezogene Daten bei der betroffenen Person erhoben, so **teilt** der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes **mit**:*

[….].

*Zusätzlich zu den Informationen gemäß Absatz 1 **stellt** der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen **zur Verfügung**, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:*

[…].

➢ Aushang im Wartezimmer vs. Aushändigung von Informationsblättern

- **KBV**:
  Aushang im Wartezimmer ist ausreichend um alle Patienten zu erreichen

- **hess. Datenschutzbeauftragter**:
  Flyer-Lösung, Aushang alleine unzureichend

- **bayerischer Datenschutzbeauftrager**:
  grundsätzlich genügt Aushang in der Praxis, auf Wunsch schriftlich aushändigen

Unterschrift des Patienten auf Informationsblatt?

- viele Arztpraxen lassen Informationsaushändigung schriftlich bestätigen
- nach Auffassung der meisten Datenschutzbehörden **nicht** erforderlich
- **aber**: Dokumentationspflicht
- **Vorsicht**: Abmahnung wegen Behandlungsverweigerung

3. Rechte der Betroffenen

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Übertragbarkeit
- Widerrufsrecht bei Einwilligung

4. Sanktionen

- Aufsichtsbehörde kann Einhaltung von Vorschriften überprüfen

Anlässe:

- Mitbewerber
- Patient
- ehemaliger Mitarbeiter

- Art. 90 DSGVO i.V.m. § 29 Abs. 3 BDSG

Berufsgeheimnisträger Ärzte/Anwälte müssen der Aufsichtsbehörde keinen Zutritt zu ihren Geschäftsräumlichkeiten gewähren, wenn dies zur Verletzung der Schweigepflicht führen würde.

➢ bei Nichteinhaltung der Vorschriften drohen Bußgelder

- Bußgelder müssen wirksam, verhältnismäßig und abschreckend sein.
- Bußgeldrahmen bis 20 Mio. Euro bzw. 4 % des Jahresumsatzes des vorangegangenen Geschäftsjahres
- Auch strafrechtliche Verfolgung möglich, sofern durch Verstoß gegen die Vorschriften die Schweigepflicht gebrochen wurde, §203 StGB.

➢ Erstes Bußgeld in Deutschland in Höhe von 20.000 € verhängt

- Hackerangriff auf Soziales Netzwerk Knuddels.de
- Daten von insgesamt 330.000 Nutzern bestehend aus Pseudonymen, Passwörtern und E-Mail-Adressen wurden erbeutet und im September veröffentlicht.
- Strafe wegen unverschlüsselter Speicherung der Daten
- Netzwerk hat Angriff direkt gemeldet

II. Aktuelle Rechtsfragen

1. Braucht meine Praxis einen Datenschutzbeauftragten?

- Art. 37 DSGVO i.V.m. **§ 38 Ziff. 1, Satz 1 BDSG neu**

Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel ***mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.***

➢ Art. 37 Abs. 1 lit. c DSGVO

die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

➢ was bedeutet „umfangreiche Verarbeitung“?

Erwägungsgrund 91 Satz 4 DSGVO

*Die Verarbeitung personenbezogener Daten sollte **nicht** als **umfangreich** gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen **einzelnen Arzt**, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.*

- **Einzelpraxis**
  muss in der Regel keinen Datenschutzbeauftragten bestellen

- **Gemeinschaftspraxis**
  sollte in der Regel einen Datenschutzbeauftragten bestellen

- **Praxisgemeinschaft**
  da getrennte Datenverarbeitung der Einzelärzte, in der Regel kein Datenschutzbeauftragter nötig

➢ § 38 Abs. 1 S. 2 BDSG

Datenschutzbeauftragter auch dann, wenn eine Datenschutz-Folgenabschätzung notwendig ist

➢ Art. 35 Abs.1 Satz 1 DSGVO

*Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich **ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge**, so führt der Verantwortliche vorab eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.*

Bestellung eines Datenschutzbeauftragen in der Arztpraxis (Übersicht)

mindestens zehn Personen ständig mit automatisierter Verarbeitung personenbezogener Daten beschäftigt (Art. 37 DSGVO i.V.m. § 38 Ziff. 1, Satz 1 BDSG neu)

ja

nein

Umfangreiche Verarbeitung Gesundheitsdaten (Art. 37 Abs. 1 lit. c DSGVO, Erwägungsgrund 91, Satz 4 DSGVO)

Nicht umfangreiche Verarbeitung Gesundheitsdaten

Datenschutzfolgenabschätzung notwendig?
(§ 38 Abs. 1 S. 2 BDSG, Art. 35 Abs.1 Satz 1 DSGVO)

Datenschutzbeauftrager (+)

Ja, wenn Datenverarbeitung gemäß Positivliste Aufsichtsbehörde z.B. Telemedizin, Apps, Videoüberwachung

nein

Datenschutzbeauftragter (-)

angesichts der Bußgeldrisiken sollte im Zweifelsfall ein Datenschutzbeauftragter benannt werden.

Hinweis: ÄK Saarland und KV Saarland bieten eine Schulung zum betrieblichen Datenschutzbeauftragten in der Arztpraxis an.

2. Auskunftsanspruch des Betroffenen Art. 15 DSGVO

- Art. 15 Abs. 1 DSGVO Auskunft, ob personenbezogene Daten verarbeitet werden.
- Wenn ja, dann Auskunft über diese Daten und **gleichzeitig** Informationen nach Art. 15 Abs. 1 lit a) bis h) über z.B. Verarbeitungszwecke, Übermittlung an Dritte, Speicherdauer usw…
- Gem. Art. 15 Abs. 3 DSGVO müssen Auskunft und erste Kopie **kostenfrei** erfolgen.
- Auskunft muss **unverzüglich**, spätestens innerhalb eines Monats erfolgen (Art.12 Abs.3 DSGVO).

Zivilrechtlicher Anspruch auf Einsichtnahme bzw. Kopie der Patientenakte

- Patientenrechtegesetz § 630g BGB bzw. § 10 Abs. 2 BO-Ä Saarland

– 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.

– Kopie der Patientenakte gegen **Kostenerstattung,** §630g Abs.2 BGB

Auskunftsanspruch Art. 15 DSGVO **vs.** **Zivilrechtlicher Anspruch auf Einsichtnahme bzw. Kopie § 630g BGB i.V.m. § 10 BO-Ä Saarland**

- Auskunftsanspruch Art. 15 DSGVO **umfassender** als Einsichtnahme § 630g BGB
- Ansprüche stehen hinsichtlich der Kostenregelung im **Widerspruch** zueinander
- Empfehlungen der Aufsichtsbehörden und Körperschaften sowie Rechtsprechung abwarten

  – ÄK Berlin: vorerst keine Kosten für Auskunft erheben
  – ÄK West-L.: beide Ansprüche stehen nebeneinander

- Da die Regelungen der DSGVO unmittelbar gelten und vorrangig vor abweichenden nationalen Regelungen anzuwenden sind (**sog. Anwendungsvorrang**), sollten vorerst keine Kosten für die Kopie der Patientenunterlagen erhoben werden.

3. Recht auf Vergessenwerden

Art. 17 Abs. 1 DSGVO

– Betroffener hat Löschungsanspruch, wenn seine personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden.

– Löschpflicht besteht unabhängig von der Aufforderung des Betroffenen.

Ausnahme von Löschpflicht Art. 17 Abs. 3 lit b DSGVO

Die Löschpflicht gilt nicht, sofern die Verarbeitung erforderlich ist zur **Erfüllung einer rechtlichen Verpflichtung**, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert.

Gesetzliche Aufbewahrungsfristen für Behandlungsunterlagen

- Berufsrechtliche Vorschrift § 10 Abs. 3 BO-Ä Saarland
- Patientenrechtegesetz § 630f Abs. 3 BGB
- Vertragsärztlicher Bereich § 57 Abs. 1 BMV-Ä

⇨ **10 Jahre nach Abschluss der Behandlung**

Solange gesetzliche Aufbewahrungsfristen laufen, hat der Betroffene keinen Löschanspruch

➢ Löschpflicht nach Ablauf der 10 Jahre?

Problem:

- Schadensersatzanspruch des Patienten aus Behandlungsfehler
- Absolute Verjährungsfrist von 30 Jahren, § 199 Abs. 2 BGB

Bayerisches Landesamt für Datenschutzaufsicht:

- Auch 30 Jährige Verjährungsfrist kann Ausnahme von Löschverpflichtung darstellen.
- Allerdings Abwägung erforderlich zwischen Interessen der Betroffenen und der Wahrscheinlichkeit der Geltendmachung von Schadensersatzansprüchen.

- Datenschutzrechtlich auf der sicheren Seite: Löschen Unterlagen nach Ablauf gesetzl. Aufbewahrungsfrist

- zwar Risiko, dass bei Arzthaftungsprozess Verteidigungsmöglichkeiten gegen Vorwurf eines Behandlungsfehlers eingeschränkt sind

- OLG Hamm (Urt. v. 29.01.2003):

  nach Ablauf der Aufbewahrungsfrist tritt keine Beweiserleichterung zugunsten des Patienten ein, wenn die Behandlungsunterlagen nicht mehr vorhanden sind.

Dürfen Patienten noch mit Namen aufgerufen werden?

- Landesdatenschutzbeauftragter **NRW**: man darf weiterhin Patienten in der Arztpraxis mit Namen ansprechen
- Landesdatenschutzbeauftragter **Bayern**: Patienten dürfen auch nach dem Inkrafttreten der DSGVO noch mit Namen aufgerufen werden.

Vielen Dank für Ihre Aufmerksamkeit!