UNIKLINIK KÖLN

Datenschutz in Gesundheitseinrichtungen

26. GQMG-Jahrestagung 2019

06.04.2019 Berlin | Dominik Zier | Datenschutzbeauftragter Uniklinik Köln

Agenda

- Personenbezogene Daten
- Besondere Kategorien personenbezogener Daten
- Rechtsgrundlagen
- Informationspflichten
- Betroffenenrechte
- Verarbeitungsdokumentation
- Einwilligung
- Entbindung von der Schweigepflicht
- Auftragsverarbeitung
- Technisch-organisatorische Maßnahmen
- Datenpannen. Dokumentations- und Informationspflichten
- Datenschutzfolgenabschätzung
- Datenschutz im Arbeitsalltag

Personenbezogene Daten (Art. 4 Abs. 1 DS-GVO)

Personenbezogene Daten sind Angaben über eine bestimmte oder bestimmbare natürliche Person.

Beispiele:

- Name
- Geburtstag
- Geschlecht
- Augenfarbe
- Einkommen
- Foto

Alle Angaben, die einer bestimmten oder bestimmbaren Person zugeordnet werden können, sind personenbezogene oder personenbeziehbare Daten!

Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO)

Besondere Kategorien personenbezogener Daten genießen einen erhöhten Schutzbedarf. Sie sind abschließend vom Gesetzgeber definiert und umfassen Angaben über die:

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben
- Genetische Daten (z.B. DNA-Analysen)
- Biometrische Daten (z.B. Fingerabdruck bei Smartphones)

Gesundheitsdaten sind immer besonders schützenswert!

Rechtsgrundlagen (Art. 6, 9 DS-GVO)

Die Verarbeitung personenbezogener Daten ist in Deutschland prinzipiell verboten („Verbot mit Erlaubnisvorbehalt“). Sie darf nur dann stattfinden, wenn

- die betroffene Person ihre Einwilligung erteilt hat (z.B. bei freiwilligen Qualitätssicherungsmaßnahmen wie Zertifizierungen oder Registerbeteiligungen).
- die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist.
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (vgl. DSGVO Art. 9, Abs. 2 lit. i), z.B. GDSG NW § 11, Abs. 2 (nur, wenn nicht anonymisiert möglich!).
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen zu schützen.
- die Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt erfolgt.
- ein berechtigtes Interesse des Verantwortlichen vorliegt (Interessenabwägung!)

Informationspflichten (Art. 13 DS-GVO)

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

- Name und Kontaktdaten des Verantwortlichen / Kontaktdaten des DSB
- Zwecke und Rechtsgrundlage der Datenverarbeitung
- Im Falle der Einwilligung Hinweis auf das Widerrufsrecht
- Ggf. Empfänger der Daten
- Bei Drittlandübermittlung Angaben zum angemessenen Datenschutzniveau
- Speicherfristen
- Aufklärung über die Betroffenenrechte / Beschwerderecht gegenüber der Aufsicht
- Herkunft der Daten, wenn nicht beim Betroffenen erhoben
- ob die Bereitstellung gesetzlich oder vertraglich vorgeschrieben ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche mögliche Folgen die Nichtbereitstellung hätte

UNIKLINIK KÖLN

Betroffenenrechte (Art. 12-23 DS-GVO)

Die von einer Datenverarbeitung betroffenen Personen haben das Recht auf

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Verarbeitung (Sperrung)
- „Nachberichtspflicht“ gegenüber Empfängern bei Berichtigung, Löschung oder Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Schutz vor Profilbildung

Verarbeitungsdokumentation (Art. 30 DS-GVO)

- Eine Verarbeitung ist ein Prozess, in dem personenbezogene Daten erhoben, verarbeitet oder genutzt werden.
- Diese Verarbeitungen müssen dokumentiert werden. Inhalt des Verzeichnisses beim Verantwortlichen:
  - Name und Kontaktdaten des Verantwortlichen und seines Vertreters
  - Kontaktdaten des Datenschutzbeauftragten
  - Rechtsgrundlage und Zwecke der Verarbeitung
  - Kategorien betroffener Personen
  - Kategorien und Löschfristen personenbezogener Daten
  - Kategorien von Empfängern und Zugriffsberechtigten
  - Übermittlung an ein Drittland einschließlich geeigneter Garantien
  - allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

Einwilligung (Art. 7 DS-GVO)

Für eine rechtskonforme Einwilligung gelten folgende Bedingungen:

- Der Verantwortliche muss nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- Erfolgt die Einwilligung durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.
- Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Sie wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
- Eine Einwilligung ist unwirksam, wenn ein Vertragsschluss oder eine Vertragserfüllung von einer Einwilligung in hierfür nicht erforderliche Verarbeitungen abhängig gemacht wird.

Entbindung von der Schweigepflicht (§ 203 Strafgesetzbuch)

- Die Schweigepflicht gilt für alle Beschäftigten einer Organisation, die mit Gesundheitsdaten eines Patienten / einer Patientin in Berührung kommen. Sie gilt nicht gegenüber internen Mitbehandlern und für konkrete Abrechnungszwecke.
- Die Schweigepflicht gilt gegenüber jedem: Angehörige und Bekannte eines Betroffenen, Berufskollegen, Vorgesetze, Familienangehörige und Freunde des Schweigepflichtigen. Sie gilt auch gegenüber Polizei, Staatsanwaltschaft und Gericht, soweit keine gesetzliche Regelung zur Offenbarung vorliegt.
- In bestimmten Fällen gibt es eine gesetzliche Auskunftspflicht, etwa gegenüber Krankenkassen oder dem medizinischen Dienst der Krankenversicherung.
- In seltenen Fällen, etwa wenn das Leben einer Person akut gefährdet ist und eine Offenlegung weiteren Schaden verhindern kann, besteht ausnahmsweise eine Offenbarungspflicht.
- Ansonsten bleibt für die Entbindung von der Schweigepflicht nur die ausdrückliche oder konkludente Einwilligung des Betroffenen.

Auftragsverarbeitung (Art. 28 DS-GVO)

Von Datenverarbeitung im Auftrag spricht man, wenn sich der Verantwortliche einer Stelle bedient, die für diese im Auftrag und weisungsabhängig personenbezogene Daten verarbeitet.

Beispiele:

- Fernwartung bei EDV-Systemen
- Vor-Ort-Wartungen durch Servicetechniker
- Ausgelagerte Datenerhebung
- Cloud-Computing (inhaltlicher Datenzugriff des Betreibers nicht erforderlich)
- Datenträgerentsorgung durch Dienstleister
- Ärztliche Verrechnungsstellen ohne Forderungsverkauf

Bei der Auftragsverarbeitung ist ein Auftragsverarbeitungsvertrag mit dem Dienstleister zu schließen. Für das Gesundheitswesen existiert ein Mustervertrag der GDD.

Abgrenzung der Auftragsverarbeitung

- Handelt der Vertragspartner frei von Weisungen und entscheidet selbst über die Zwecke und Mittel der Datenverarbeitung, kann kein Auftragsverarbeitungsvertrag abgeschlossen werden.
- Ohne einen wirksamen Auftragsverarbeitungsvertrag bedarf die Übermittlung der personenbezogenen Daten an einen Dritten einer Rechtsgrundlage.
- Gemäß Art. 26 Abs. 1 DS-GVO können auch mehrere Stellen „gemeinsam für die Verarbeitung Verantwortliche“ sein, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.

Beispiele:

- Tätigkeiten von Berufsgeheimnisträgern
- Fertigung individueller medizinischer Produkte, Hilfsmittel, Prothesen
- Postdienstleister für den Brief- oder Pakettransport
- Übersetzen von Texten in / aus Fremdsprachen

Technisch-organisatorische Maßnahmen

Technisch-organisatorische Maßnahmen gewährleisten den Schutz personenbezogener Daten und Informationen:

- Zutrittskontrolle (Ausweisleser, Schlüssel, Pförtner, Videoüberwachung)
- Zugangskontrolle (Passwörter, automatische Sperrung, Verschlüsselung Datenträger)
- Zugriffskontrolle (Rechte und Rollen, Auswertungen)
- Weitergabekontrolle (VPN, Verschlüsselung, Transportsicherung)
- Eingabekontrolle (Protokollierung, Auswertungen)
- Auftragskontrolle (Formular AV UKK verwenden, Kontrolle der TOM des Dienstleisters)
- Verfügbarkeitskontrolle (Backup, USV, getrennte Aufbewahrung, Virenschutz)
- Trennungskontrolle (Mandantenfähigkeit, Zweckbindung)

-> es gilt das Prinzip der Verhältnismäßigkeit!

Datenpannen. Dokumentations- und Informationspflichten (Art. 33f. DS-GVO)

- Datenpannen bezeichnen einen Vorfall, bei dem z.B. Unberechtigte Zugriff auf eine Datensammlung erhalten (Falscher Faxempfänger, Befunde im Hausmüll entsorgt, verlorener, unverschlüsselter USB-Stick)
- Datenpannen sind grundsätzlich innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde zu melden.
- Darüber hinaus besteht eine Informationspflicht gegenüber den Betroffenen, wenn die Datenschutzverletzung zu einem hohen Risiko für den Betroffenen führt
- Ausnahme: „… es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt.“
- Selbst wenn nicht gemeldet werden muss, besteht eine interne Dokumentationspflicht zu jedem Datenschutzverstoß.
- Es sollte eine zentrale E-Mail-Adresse zur Meldung von Datenpannen zur Verfügung gestellt werden.

Datenschutzfolgenabschätzung (Art. 35 DSGVO)

- Ist immer dann durchzuführen, wenn eine Verarbeitung ein hohes Datenschutzrisiko zur Folge hat:
  - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
  - umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- Diese Kriterien werden in WP 248 der Art.-29-Gruppe weiter konkretisiert.
- Positivlisten der Aufsichtsbehörden
- Umsetzungshilfen: Kurzpapier der DSK, Tool der CNIL

Datenschutz im Arbeitsalltag

Hinweise für einen gelebten Datenschutz:

- Rechner sperren (Windowstaste + „L“) beim Verlassen des Arbeitsplatzes
- Clean Desk nach Dienstschluss
- Keine Unterlagen im Drucker oder Faxgerät liegen lassen
- Papierentsorgung in Datenschutztonnen
- Keine Nutzung von WhatsApp oder anderen Messengern
- Faxe an Kurzwahlnummern senden
- Sensible Daten per E-Mail immer verschlüsselt versenden
- Nur verschlüsselte Datenträger verwenden

Vielen Dank!

UNIKLINIK KÖLN