gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Rechtliche Grundlagen

des Datenschutzes nach DS-GVO

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Agenda

- EU-Recht, Bundes- und Landesrecht, Kirchenrecht
  - wann gilt was?
- Grundsätze des Datenschutzes
- Rechtsmäßigkeit der Datenverarbeitung
  - Verbot mit Erlaubnisvorbehalt
- Was sind personenbezogene Daten?
  - besondere Kategorien von personenbezogenen Daten, Gesundheitsdaten und Genomdaten
- Unterschied anonym und pseudonym
- Verantwortlicher, Auftragsverarbeiter, Empfänger, Dritter
- Verantwortlicher für die Verarbeitung
- Gemeinsam Verantwortliche

EU-Recht, Bundes-, Landes- und Kirchenrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Landesdatenschutzgesetze

Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein, Thüringen

→ Landesbeauftragte für den Datenschutz

→ Bayern: Bayr.LDSB + Landesamt für Datenschutzaufsicht

Datenschutz in Redaktionen

Selbstkontrolle

→ Deutscher Presserat

Datenschutz in Rundfunkanstalten

Selbstkontrolle

→ Rundfunkdatenschutzbeauftragte

Kirchen

→ Kirchendatenschutzbeauftragte

Öffentlicher Bereich des Bundes

→ Bundesbeauftragte f. d. Datenschutz

Privatwirtschaft

Aufsichtsbehörden der Länder

Ergänzende Gesetze

Geltungsbereich	Krankenhausgesetze
Bund und bundesweit	Krankenhausfinanzierungsgesetz - KHG Sozialgesetzbuch – SGB V; SGB VI; SGB IX; SGB X
Baden-Württemberg	Landeskrankenhausgesetz Baden-Württemberg (LKHG)
Bayern	Bayerisches Krankenhausgesetz (BayKrG)
Berlin	Landeskrankenhausgesetz (LKG)
Brandenburg	Brandenburgisches KH-Entwicklungsgesetz- BbgKHEG
Bremen	Bremisches Krankenhausdatenschutzgesetz (BremKHDSG)
Hamburg	Hamburgisches Krankenhausgesetz (HmbKHG)
Hessen	Hessisches Krankenhausgesetz 2011 - HKHG 2011
Mecklenburg-Vorpommern	Landeskrankenhausgesetz LKHG M-V
Niedersachsen	Niedersächsisches Krankenhausgesetz (NKHG) – ohne DS!
Nordrhein-Westfalen	Gesundheitsdatenschutzgesetz - GDSG NW
Rheinland-Pfalz	Landeskrankenhausgesetz (LKG)
Saarland	Saarländisches Krankenhausgesetz
Sachsen	Sächsisches Krankenhausgesetz (SächsKHG)
Sachsen-Anhalt	Krankenhausgesetz Sachsen-Anhalt (KHG LSA) – ohne DS!
Schleswig-Holstein	Kein Landeskrankenhausgesetz ! – keine DS-Regelung!
Thüringen	Thüringer Krankenhausgesetz (ThürKHG)

Ergänzende Gesetze

Geltungsbereich	Krankenhausgesetze
Katholische Kirche	Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern im Erzbistum Hamburg, Bistum Hildesheim, Bistum Osnabrück, Oldenburgischen Teil des Bistums Münster
Evangelische Kirche	Verordnung zum Schutz Patientendaten in kirchlichen Krankenhäusern, Vorsorge- und Rehabilitationseinrichtungen (DSVO-KH)

Grundsätze des Datenschutzes

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Personenbezog. Daten müssen und dürfen nur

- rechtmäßig, richtig, angemessen sicher
- auf konkret festgelegte legitime Zwecke
- mit umfassender Kenntnis des Betroffenen
- und nur so lange wie notwendig

verarbeitet werden.

Der Verantwortliche muss die Einhaltung des Datenschutzes **nachweisen** können.

→ Artikel 5 DSGVO

Rechtmäßigkeit der Datenverarbeitung

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

„Verbot im Erlaubnisvorbehalt“
bei nicht sensitiven Daten !

Die Verarbeitung ist NUR rechtmäßig, wenn (entweder/oder)

- der Betroffene eingewilligt hat
- ein Vorvertrag oder Vertrag zugrunde liegt
- rechtliche Verpflichtungen diese bestimmt
- lebenswichtige Interessen diese erfordern
- sie im öffentlichen Interesse auftragsgemäß durchgeführt wird
- sie zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritten erforderlich ist und das Recht Betroffener nicht überwiegen

→ Artikel 6 DSGVO

Verarbeitung besonderer Kategorien p.b. Daten → Art 9 DSGVO

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Die Verarbeitung p.b. Daten, …sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten …. ist untersagt.
- Das gilt jedoch nicht, wenn
  - die betroffene Person in die Verarbeitung … ausdrücklich eingewilligt hat
  - die Verarbeitung zum Schutz lebenswichtiger Interessen …. erforderlich und die betroffene Person …. außerstande ist, ihre Einwilligung zu geben,
  - die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich ….. aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich ist
- … diese Daten dürfen von Fachpersonal oder unter dessen Verantwortung verarbeitet werden, wenn dieses dem Berufsgeheimnis unterliegt
- Die Mitgliedsstaaten können zusätzliche Bedingungen … einführen, soweit die Verarbeitung von genetischen, biologischen oder Gesundheitsdaten betroffen ist

„Verarbeitung“ und „Dateisystem“

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Verarbeitung

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

Dateisystem

jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird

→ Artikel 4 DSGVO

Was sind personenbezogene Daten?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Betroffener = natürliche identifizierte oder identifizierbare Person
- Gesundheitsdaten
  - beziehen sich auf die körperliche oder geistige Gesundheit, einschließlich der Erbringung von Gesundheitsdienstleistungen, und aus denen Informationen über deren Gesundheitszustand hervorgehen;
- biometrische Daten
  - Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen (z.B. Gesichtsbilder, daktyloskopische Daten)
- genetische Daten
  - genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden

→ Artikel 4 DSGVO

Unterschied anonym und pseudonym

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- personenbezogene Daten = natürliche Person = betroffene Person
  - alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
  - als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels … Namen, … einer Kennnummer, … Standort-daten, … Online-Kennung oder …. Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirt-schaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind
- Pseudonym:
  - p.b. Daten, die durch Heranziehung zusätzlicher Informationen einer natür-lichen Person zugeordnet werden könnten. Dabei ist es unerheblich, ob der Nutzer dieser Daten über diese zusätzlichen Informationen verfügt.
  - EWG 26: Einer Pseudonymisierung unterzogene p.b. Daten, die durch Heran-ziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natür-liche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren….

- Anonym:
  - Informationen, durch die betroffene Person nicht oder nicht mehr identifiziert werden können
  - § 27 (3) BDSG (neu): …Sinne des Artikels 9 Absatz 1 sind p.b. Daten zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist…
  - EWG 26: Die Grundsätze des Datenschutzes gelten nicht für anonyme Informationen

→ Artikel 4 und EWG 26 DSGVO; § 27 (3) BDSG (neu)

Verantwortlicher, Auftrags-verarbeiter, Empfänger, Dritter

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Verantwortlicher
  - die natürliche oder juristische Person … oder Stelle, die ….. über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
- Auftragsverarbeiter
  - eine natürliche oder juristische Person … oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
- Empfänger
  - eine natürliche oder juristische Person … oder Stelle, denen personen-bezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht
- Dritter
  - eine natürliche oder juristische Person … oder Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten

→ Artikel 4 DSGVO

Verantwortlicher für die Verarbeitung

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

- Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen die Anwendung geeigneter Datenschutz-vorkehrungen durch den Verantwortlichen umfassen.

- Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

→ Artikel 24 DSGVO

Gemeinsam Verantwortliche

„kleines Konzernprivileg“

- Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt….. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

- Die Vereinbarung …muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

- …. die betroffene Person / kann / ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

→ Artikel 26 DSGVO

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Haben Sie dazu noch Fragen ?