UKD Universitätsklinikum Düsseldorf

GKD Gesellschaft für klinische Dienstleistungen Düsseldorf mbH

Datenschutzrechtliche Anforderungen an medizinische Portallösungen

Was ist Datenschutz?

1. Datenschutz ≠ Schutz der Daten
2. Datenschutz = Schutz der Freiheit einer Person, selbst zu entscheiden, was mit ihren/seinen Daten geschieht

Was ist Datenschutz?

Die Person soll selbst entscheiden, was mit ihren Daten geschieht:

- Datenschutz ist überall dort vorhanden, wo eine ***asymmetrische Machtbeziehung*** zwischen Personen und Organisationen existiert:
  - Öffentliche Verwaltung und Bürger
  - Private Unternehmen und Kunden
  - Arbeitgeber und Arbeitnehmer
  - **Praxen, Krankenhäuser und Patienten**
  - Institute, Gemeinschaften und Mandanten
  - Wissenschaftsorganisationen und Forschungspobjekte (wenn diese Menschen darstellen)
  - Verein und Mitglieder
  - Schule und Schüler
  - …

Internet-„Portale“

Telemediengesetz, § 1 Anwendungsbereich, Abs. 1:

- Dieses Gesetz gilt für alle
  - **elektronischen Informations- und Kommunikationsdienste**,
    - soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien).
  - Dieses Gesetz gilt für **alle Anbieter** einschließlich der öffentlichen Stellen **unabhängig davon**, **ob für die Nutzung ein Entgelt erhoben wird.**

Internet-„Portale“

Es gilt

- Datenschutzrecht (Landes-/Bundesrecht)
- TMG
- TKG

Kurz: das sogenannte „3-Schichten-Modell“:

3-Schichten-Modell

Schicht 3	Bedeutungs- oder Inhaltsebene 2 Akteure treten miteinander in Beziehung: Eine Person als „Abfrager“, eine Organisation als „Anbieter“
Schicht 2	Interaktionsebene eines Nutzers mit der Technik Der Abfrager nutzt Internetdienst (E-Mail, Web, …) mittels Menüs, Buttons, Eingabefeldern und Links des Anbieters
Schicht 1	Telekommunikationsebene Diese Ebene umfasst also Aspekte der Netzwerktechnik bzw. des Datentransports

3(7)-Schichten-Modell

OSI-Modell		Anzuwendende Gesetze
7	Anwendung	(Gesundheits)- Datenschutzgesetze (Bundesrecht / Landesrecht / Kirchenrecht / AGBs)
6	Darstellung	Telemediengesetz
5	Sitzung	
4	Transport	Telekommunikationsgesetz
3	Vermittlung	
2	Sicherung	
1	Bitübertragung	

3(7)-Schichten-Modell: Beispiel

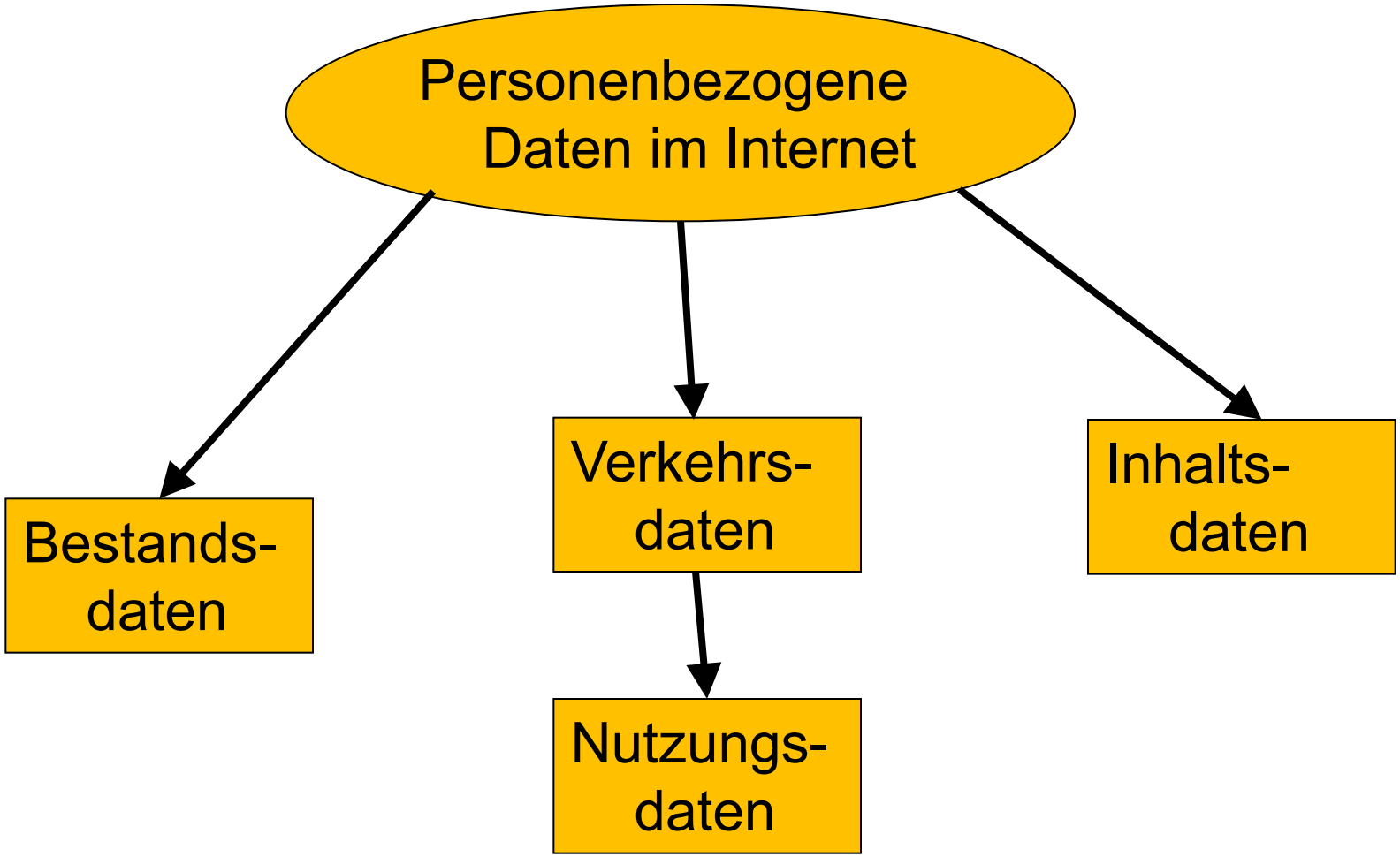
OSI-Modell		Anzuwendende Gesetze
7	Anwendung	Online-Banking, Überweisung: Betrag, Empfänger,...
6	Darstellung	Online-Banking: Login-Daten, Benutzername, Passwort
5	Sitzung	
4	Transport	Online-Banking: IP-Adresse, OS, ...
3	Vermittlung	
2	Sicherung	
1	Bitübertragung	

Datenschutzgesetze

- EU
  - Europäische Grundrechte-Charta
  - Datenschutz-Richtlinie
    Wirkung über Umsetzung in deutsche Gesetze
  - Datenschutz-Verordnung
    (derzeit im Entwurf, sie würde unmittelbar gelten und deutsches Recht ersetzen)
- Bundesdatenschutzgesetz (BDSG)
  - Privatpersonen
  - Privatwirtschaft
  - Bundesbehörden
- Kirchliche Datenschutzgesetze
  - Einrichtungen der evang. und kath. Kirche
- Landesdatenschutzgesetze
  - öffentliche Verwaltung in Land und Kommunen
- Spezialgesetze
  (Vorrang vor allg. Gesetzen)
  - TeleMedienGesetz
  - TeleKommunikationsGesetz
  - Gesundheitsdatenschutz
  - Sozialgesetzbuch
  - Hochschulgesetz
  - SGB, AO, Polizeigesetz, Passgesetz, Personalausweisgesetz, Aufenthaltsgesetz, LandesMeldeGesetz, Landesverwaltungsgsetz, …

- Rechtmäßigkeit der Datenverarbeitung
  - Gesetzliche Grundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeiten
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- Nutzung pseudonymisierter oder anonymisierter Daten
- Verpflichtung zum Schutz der Daten

Telemedienrecht – Grundlegende Begriffe



Telemedienrecht – Grundlegende Begriffe

- Bestandsdaten:
  Daten zur Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses zwischen dem Anbieter und dem Nutzer einer Internetdienstleistung erhoben werden. Beispiele:
  Name, Adresse, Log-In-Kennung, Bankverbindungsdaten.
- Verkehrsdaten:
  Daten, die „bei der Erbringung eines Dienstes“ erhoben, verarbeitet oder genutzt werden. Umfasst sind: wer hat wann, wo (bzw. bei Festnetz von welchem Anschluss aus) mit wem kommuniziert oder versucht zu kommunizieren.
- Nutzungsdaten:
  Daten, die der Anbieter benötigt, um die Inanspruchnahme seines Dienstes zu ermöglichen und abzurechnen.Umfasst sein können insbesondere: Identifikation des Nutzers (IP-Adresse), Beginn und Ende der jeweiligen Nutzung, Angaben über die in Anspruch genommenen Medien.
- Inhaltsdaten:
  Sind Daten, die den Inhalt einer Kommunikation betreffen.

Datenschutzgesetz vs. Telemediengesetz / Telekommunikationsrecht

Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) sind als bereichsspezifisches Recht dem allgemeinen Datenschutzgesetz vorrangig!

Merke:

Die Vertraulichkeit der Kommunikation ist regelmäßig **grundrechtlich** durch das Fernmeldegeheimnis aus **Art. 10 Abs. 1 GG** besonders geschützt!

TMG

Abschnitt 4

Datenschutz

- § 11 Anbieter-Nutzer-Verhältnis
- § 12 Grundsätze
- § 13 Pflichten des Diensteanbieters
- § 14 Bestandsdaten
- § 15 Nutzungsdaten
- § 15a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

TMG

- Rechtsgrundlage / Einwilligung des Betroffenen
  (nicht notwendigerweise des Patienten!)
  (§12 Abs. 1)
- Nutzer des Webdienstes muss informiert sein, Einwilligung muss vorliegen (§13 Abs.1 und 2)
- Datenschutzhinweise müssen in allgemein verständlicher Form, leicht erkennbar und unmittelbar erreichbar sein (§13 Abs.1)
- Umsetzung TOV (§13 Abs. 4)
- Auskunft über Bestandsdaten für Zwecke der Strafverfolgung und Gefahrenabwehr (§14 Abs. 2)
- Grundsatz: Anonyme und pseudonyme Nutzung ist zu ermöglichen, soweit „technisch möglich und zumutbar“ (§ 13 Abs. 6 TMG)

Einwilligung TMG / TKG

Die Einwilligung kann auch elektronisch erklärt werden, wenn gewährleistet ist, dass

1. der Teilnehmer oder Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann

Technische und organisatorische Vorkehrungen im Sinne des TMG

Der Anbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
5. zur Abrechnung benötigte Daten nur für Abrechnungszwecke zusammengeführt werden können und
6. Nutzungsprofile nach nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

TMG: sonstiges

- Pflicht zu allgemeinen Informationen zum Anbieter (Impressum), §§ 5, 6 TMG
- Unterrichtungspflichten zu Beginn des Nutzungsvorgangs, § 13 Abs. 1 TMG
- Eingeschränkte Verantwortlichkeit für Inhalte, die sie für „fremde“ Nutzer speichern, § 7, §§ 8-10 TMG
- Relativ strenge Zweckbindung, §§ 12, 14, 15 TMG
- Regelungen zur Einwilligung: „Opt-In“, § 13 Abs. 2 TMG

Telekommunikationsgesetz (TKG)

Abschnitt 2

Datenschutz

- § 91 Anwendungsbereich
- § 92 (weggefallen)
- § 93 Informationspflichten
- § 94 Einwilligung im elektronischen Verfahren
- § 95 Vertragsverhältnisse
- § 96 Verkehrsdaten
- § 97 Entgeltermittlung und Entgeltabrechnung
- § 98 Standortdaten
- § 99 Einzelverbindungsnachweis
- § 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten
- § 101 Mitteilen ankommender Verbindungen
- § 102 Rufnummernanzeige und -unterdrückung
- § 103 Automatische Anrufweiterschaltung
- § 104 Teilnehmerverzeichnisse
- § 105 Auskunftserteilung
- § 106 Telegrammdienst
- § 107 Nachrichtenübermittlungssysteme mit Zwischenspeicherung

Informationspflichten des TKG

- Teilnehmer bei Vertragsabschluss über
  - Art,
  - Umfang,
  - Ort und
  - Zweck

  der Erhebung und Verwendung personenbezogener Daten unterrichten
- Teilnehmer auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinweisen
- Teilnehmer über Risiko der Verletzung der Netzsicherheit hinweisen
- Unterrichtung Teilnehmer im Fall Verletzung des Schutzes personenbezogener Daten

TKG und Teilnehmerverzeichnisse

§104 TKG Teilnehmerverzeichnisse

- Teilnehmer **können** mit
  - ihrem Namen,
  - ihrer Anschrift und
  - zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses

  in öffentliche gedruckte oder elektronische Verzeichnisse eingetragen werden, soweit sie dies beantragen.
- Dabei **können** die Teilnehmer bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen.
- Auf Verlangen des Teilnehmers **dürfen** Mitbenutzer eingetragen werden, soweit diese damit

§105 TKG Auskunftserteilung

- Über in Teilnehmerverzeichnissen enthaltene Rufnummern darf eine Auskunft erteilt werden

Sanktionen: Ordnungswidrigkeiten / Bußgelder

- Fehlende Bestellung eines Datenschutzbeauftragten
- Fehlende Vorabkontrolle bei Datenübermittlung
- Fehlender Vertrag zur Auftragsdatenverarbeitung
- Fehlende Information bei Nutzung von Daten für Adresshandel oder Werbung
- Datenübermittlung ohne rechtliche Grundlage oder Einverständniserklärung
- Unvollständige Bearbeitung des Auskunftersuchens eines Betroffenen
- Daten werden auf Aufforderung nicht korrigiert oder gelöscht
- Fehlende/unvollständige Information der zuständigen Aufsichtsbehörde

= Geldbuße bis zu 50.000 Euro
Aber: Geldbuße soll den wirtschaftlichen Vorteil übersteigen; bei Bedarf kann Betrag überschritten werden

Sanktionen: Ordnungswidrigkeiten / Bußgelder

- Unbefugte Erhebung oder Verarbeitung nicht allgemein zugänglicher Daten
- Nicht allgemein zugängliche Daten unbefugt per automatisierten Abrufverfahren bereitstellen
- Unbefugte Beschaffung nicht allgemein zugänglicher Daten abrufen oder automatisiert beschaffen
- Unbefugte Übermittlung nicht allgemein zugänglicher Daten
- Vertragsabschluss nur in Abhängigkeit von der Zustimmung zum Adresshandel und/oder Werbung
- Nutzung von nicht allgemein zugänglichen Daten zu Adresshandel, Werbung oder Markt-, Meinungsforschung trotz Widerspruch des Betroffenen
- Unzureichende Anonymisierung bei geschäftsmäßiger Datenverarbeitung mit Übermittlung in anonymisierter Form
- Bei Datenpannen den Betroffenen nicht oder nur unvollständig informiert

= Geldbuße bis zu 300.000 Euro
Aber: Geldbuße soll den wirtschaftlichen Vorteil übersteigen; bei Bedarf kann Betrag überschritten werden

Sanktionen: Straftatbestand

Wer vorsätzlich gegen Entgelt oder in der Absicht sich oder einen anderen zu bereichern oder einen anderen zu schädigen:

- Unbefugte Erhebung oder Verarbeitung nicht allgemein zugänglicher Daten
- Nicht allgemein zugängliche Daten unbefugt per automatisierten Abrufverfahren bereitstellen
- Unbefugte Beschaffung nicht allgemein zugänglicher Daten abrufen oder automatisiert beschaffen
- Unbefugte Übermittlung nicht allgemein zugänglicher Daten
- Vertragsabschluss nur in Abhängigkeit von der Zustimmung zum Adresshandel und/oder Werbung
- Nutzung von nicht allgemein zugänglichen Daten zu Adresshandel, Werbung oder Markt-, Meinungsforschung trotz Widerspruch des Betroffenen
- Unzureichende Anonymisierung bei geschäftsmäßiger Datenverarbeitung mit Übermittlung in anonymisierter Form
- Bei Datenpannen den Betroffenen nicht oder nur unvollständig informiert

= Freiheitsstrafe bis zu 2 Jahre oder Geldstrafe

- Tat wird nur auf Antrag verfolgt
- Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, die Aufsichtsbehörde, der Bundesdatenschutzbeauftragte

Fazit

- Zweckbindung beachten
- Einwilligung Nutzer und Patient muss vorliegen (Opt-In beachten)
- Umsetzung technische und organisatorische Vorkehrungen TMG
- Ggfs. Bestandsdaten für Strafverfolgung vorrätig halten
- Informationspflichten TKG beachten
- Und natürlich: Anforderungen der Datenschutzgesetze

Diskussion


Vereinfachen Sie Ihre Kommunikation:
Hmmm...
ääh...
räuspert...
(schluck!)
Nein.
Ich denke...
Man könnte...
unter Umständen...
möglicherweise...
...denkbar wäre...
Ja.