Datenschutzrecht

Datenverarbeitung im Auftrag

Medizindatenschutz, Berufsgeheimnisträger

4. Dezember 2023

Harald Zwingelberg

Ansprechpartner Vorlesungsreihe: Benjamin Bremert

Vertretene Auffassungen sind solche des Referenten bzw. teilweise Ergebnisse aus dem Forschungs- und Projektbereich und kann von den Auffassungen der Datenschutz-Aufsichtsbehörde(n) abweichen.

Ankündigungen

- Gesetzestexte für Vorbereitung und Klausur:
  - DSGVO (insbesondere Art. 1-40)
  - https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
  - Druckfassung bereitgestellt: https://www.datenschutzzentrum.de/uploads/vorlesungen/cau/Gesetzessammlung.pdf

- Soweit nicht anders gekennzeichnet, sind alle genannten Artikel solche der DSGVO.

Agenda

- Wiederholung:
  - Grundprinzipien,
  - personenbezogene Daten
  - besondere Kategorien personenbezogener Daten
- Gesundheitsdatenschutz
- Datenschutz und Forschung

Wiederholung

Grundlagen

Wiederholung

- Wo sind die Grundprinzipien des Datenschutzes geregelt?
  - Art. 5 DSGVO

- Nennen sie die Grundprinzipien und deren Kerninhalt
  1. Rechtmäßigkeit, Art. 5 I a
  2. Zweckbindung, Art. 5. I b
  3. Erforderlichkeit, Art. 5 I b, c (u.a. Datenminimierung)
  4. Transparenz, Art. 5 I a (Auskunft, …)
  5. Integrität und Vertraulichkeit (Datensicherheit), Art. 5 I f
  6. Rechenschaftspflicht, Art. 5 II

*Wiederholung *)*
Sechs Goldene Regeln des Datenschutzes

Welche Grundsätze des Datenschutzes kennen Sie?

- Rechtmäßigkeit
  - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- Zweckbindung
  - Weiterverarbeitung nur für einem mit Erhebungszweck vereinbaren Zweck
- Datenminimierung und Speicherbegrenzung
  - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz und Betroffenenrechte
  - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- Integrität und Vertrautlichkeit
  - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- Kontrolle
  - Interner / externer Datenschutzbeauftragter

*) Zum ganzen siehe Einführung von B. Bremert vom
Ausführlich zu Data Protection Principles, B. Bruegger,
http://guidelines.panelfit.eu/the-gdpr/main-principles/

Wiederholung
Art. 6 DSGVO: Zentrale Befugnisnorm

- Datenverarbeitung ist (nur!) rechtmäßig, wenn:
  - **Einwilligung**
  - **Vertragserfüllung**
  - **Erfüllung rechtlicher Verpflichtung**
  - Lebenswichtige Interessen
  - Ausübung öffentliche Gewalt
  - **Wahrung berechtigter Interessen, sofern Interessen des Betroffenen nicht überwiegen *)**

*) Ausführlich zur Verarbeitung für berechtigte Interessen nach Art. 6 I f DSGVO:
Robrahn/Bremert, Interessenskonflikte im Datenschutzrecht, ZD 2018, 291ff.
Autorenversion frei verfügbar :
https://www.datenschutzzentrum.de/uploads/projekte/itesa/Robrahn-Bremert-Artikel6abs1fDSGVO.pdf

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

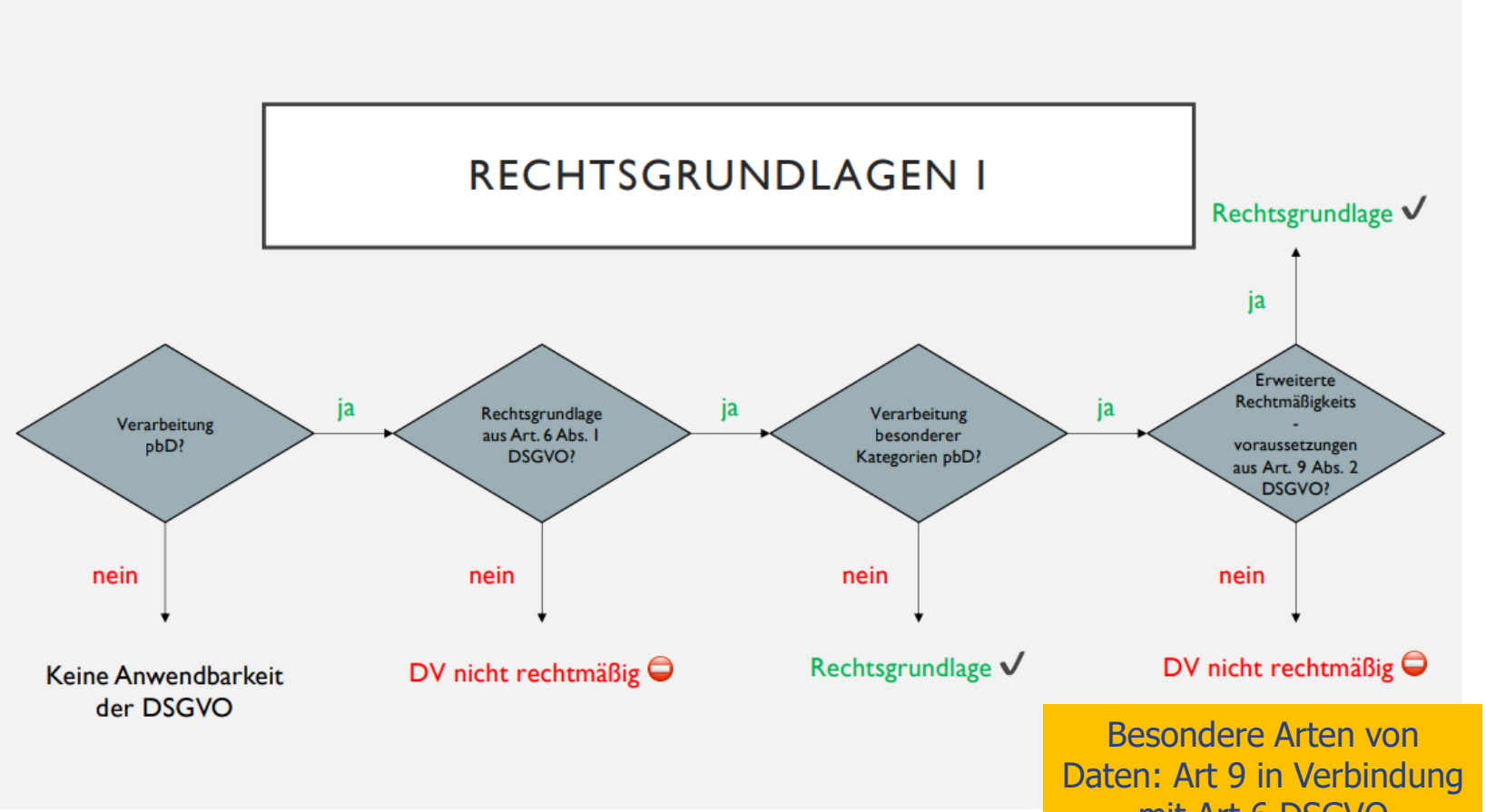
iTESA

Wiederholung
Besondere Kategorien personenbez. Daten

- Art. 9 (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 nat. Person ist untersagt.

- Art 9 (2) DSGVO: Ausnahmen vom Verbot u.a. für Behanldung und Forschung

Rechtsgrundlagen Wiedergholung



Besondere Arten von Daten: Art 9 in Verbindung mit Art 6 DSGVO

Quelle der Folie: Benjamin Bremert, zur wiederholung siehe Veranstaltung „Einfühung II" vom

Auftragsverarbeitung

Auftragsverarbeitung als rechtliche Gestaltungsmöglichkeit

Anforderungen, Umfang, Rechtsfolgen

Auftragsdatenverarbeitung Anwendungsbereich, Bedeutung

Problemstellung

- Relevante Grundsätze des Datenschutzrechts:
  - Rechtmäßigkeit, Art. 5 (1) DSGVO daher sind erforderlich:
    - Einwilligung, Art. 6 (1) (a) oder
    - anderweitige gesetzliche Rechtsgrundlage, Art. 6 (1) …
  - Datensicherheit

Folge

- Bei jedem Datenfluss ist grundsätzlich zu prüfen, ob es einer Rechtsgrundlage (RGL) für die Übermittlung bedarf und die Sicherheit der Verarbeitung ist zu gewährleisten.
- Erhebung durch Dritten bedarf eigener RGL für Empfänger.

Auftragsdatenverarbeitung Anwendungsbereich, Bedeutung

- Typische Anwendungsbereiche der Auftragsverarbeitung
  - Hosting (insbesondere mit Webshop und Kundendaten),
  - externe Datensicherung,
  - IT-Betreuung, soweit Zugriff auf personenbez. Daten besteht,
  - Aktenvernichtung,
  - Druck- und Versandleistungen (Lettershop),
  - Lohnbuchhaltung,
  - Callcenter,
  - Kundenservice durch Service-Partner
  - …

Auftragsdatenverarbeitung Definitionen

Begriffsbestimmungen für Akteure der Datenverarbeitung

- Art. 4 (7) DSDGVO: ***Verantwortlicher*** ist die [Einrichtung], die allein oder gemeinsam mit anderen Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet… (Engl.: controller)

- Art. 4 (8) DSGVO: ***Auftragsverarbeiter*** ist eine [Einrichtung] die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Eng.: processor)

- Art. 26 (1) DSGVO: ***Gemeinsam Verantwortliche***: Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, sind sie gemeinsam Verantwortliche. (Engl.: joint controllers)
  - Zentraler Punkt in jüngeren EuGH-Urteilen: Gemeinsam Verantwortliche sind ein Webseitenbetreiber, der mittels Einbindung eines Social-Media-Plugins auf der eigenen Webseite (EuGH 2019, Fashion ID, C-40/17, Rn. 81) oder mittels Nutzung eine Fanpage (EuGH 2018, Wirtschaftsakademie, C-210/16, Rn. 39) Datenflüsse an den Plattformbetreiber veranlasst.

Auftragsdatenverarbeitung Voraussetzungen

Voraussetzungen Art. 28 DSGVO

- völlige Weisungsabhängigkeit des Auftragsverarbeiters
- Vertrag mit bestimmten Mindestinhalten, Art. 28 (3) – Teil 1
  - Art und Zweck der Verarbeitung, Dauer, Art der personenbezogenen Daten, Kategorien betroffener Personen
  - Bindung des Auftragsverarbeiters an Weisungen des Verantwortlichen
  - Pflichten und Rechte des Verantwortlichen gegenüber dem Auftragsverarbeiter
  - Verarbeitung nur auf Basis dokumentierter Weisung des Verantwortlichen Besteht ausnahmsweise eine Rechtspflicht des Auftragsverarbeiters zur Übermittlung an Dritte muss der Auftragsverarbeiter diese rechtlichen Rahmenbedingungen vor der Verarbeitung dem verantwortlichen mitteilen. lit. a)
  - Mitarbeiter des Auftragsverarbeiters müssen zur Vertraulichkeit verpflichtet werden. lit b)

Auftragsdatenverarbeitung Voraussetzungen

Voraussetzungen Art. 28 DSGVO

- Vertrag mit bestimmten Mindestinhalten, Art. 28 (3) – Teil 2 (Fortsetzung)
  - Erforderliche techn.-org. Maßnahmen nach Art. 32 sind zu treffen. lit c)
  - Auflagen bei der Inanspruchnahme von (Unter-)Auftragsverarbeitern durch den Auftragsverarbeiter. lit. d)
  - Unterstützung des Verantwortlichen bei der Gewährung von Betroffenenrechten
  - Löschung oder Rückgabe aller Daten nach Abschluss der Verarbeitung
  - Überlassen der nötigen Informationen, um die Einhaltung der Vorschriften auch gegenüber Prüfern nachzuweisen
- Der Vertrag kann auch in Textform (online) geschlossen werden. Schriftform ist nicht mehr erforderlich.

Auftragsdatenverarbeitung Voraussetzungen

Art. 28 als eigenständige Rechtsgrundlage?

Muss neben Art. 28 zusätzlich eine Rechtsgrundlage aus Art. 6 gegeben sein?

- Antwort: Nein, Art. 28 ist Rechtsgrundlage für die Verarbeitung im Rahmen einer Auftrags-DV. Daneben sind entsprechend die weiteren Voraussetzungen der DSGVO einzuhalten, z.B. bei technisch-organisatorischen Maßnahmen.
  Grund: Auftragnehmer wird als quasi-interne Stelle des Verantwortlichen behandelt. Die Trennung macht nur Sinn, wenn mit Einhalten der Anforderungen nicht zusätzlich eine RGL bestehen müsste. Ansonsten würde ja bereits die RGL den Datenfluss ohne Extra-Aufwand gestatten.

Auftragsdatenverarbeitung Abgrenzung

Abgrenzung von (gemeinsam) Verantwortlichen

- Bei (gemeinsam) Verantwortlichen hat der Ausführende die Entscheidung über Zwecke und Mittel der Datenverarbeitung. Eigenverantwortlichkeit und eingeschränkte Entscheidungsbefugnisse bei der Durchführung lassen nicht automatisch eine Auftrags-DV ausscheiden (nicht-wesentliche Mittel).
- Für Auftragsverarbeitung sprechen besonders ausführliche Weisungen, engmaschige Überwachung oder wenn der Auftragsverarbeiter den Eindruck erweckt, er gehöre organisatorisch zum Verantwortlichen.
- Umgekehrt haben insbesondere einige freie Berufe auf Grundlage der Berufsordnungen eigenständige Rechtsgrundlagen für die Verarbeitung, da diese nur Teil einer umfassenderen Beratungsfunktion gegenüber Ihren Kunden (Mandanten, Patienten) ist. Beispiele Rechtsanwälte, Steuerberater, Psychologen… Diese sind dann Verantwortliche.
- Quellen: EDSA, Guidelines 07/2020 v2 on the concepts of controller and processor in the GDPR.

Auftragsdatenverarbeitung Abgrenzung

Abgrenzung am Beispiel eines Telefon- und Mailanbieters

(?) Wie ist abzugrenzen? Welche Kernfrage ist vorab zu klären?

Abgrenzungsfrage: Um welche Datenverarbeitungen geht es?

- Datenverarbeitung für Verbindungsaufbau, Rechnungsstellung, Systemwartung: Für diese Daten ist der TK-Anbieter Verantwortlicher im Sinne der DSGVO

- Inhalte der Datenübermittlung:
  Der TK-Anbieter wird nicht Verantwortlicher. Das bleiben die an der Kommunikation Beteiligten.

⇒ Merke: Es kommt auf die jeweilige Verarbeitungstätigkeit an. Es ist auch möglich für eine Verarbeitung (Mit-)Verantwortlicher zu sein für eine andere nur Auftragnehmer.

Quelle: EDSA, Leitlinie 07/2020 Version 2, Rn. 27.

Auftragsdatenverarbeitung Pflichten

Pflichten / Aufgaben des Verantwortlichen

- Sorgfältige Auswahl und Überwachung nach Art. 28
- Vertragliche Bindung
- Bereitstellung der erforderlichen Informationen für den Auftragsverarbeiter

Pflichten des Auftragsverarbeiters

- Bei Sitz im Drittland – Bestellung eines Vertreters in der Union, Art. 27
- Verzeichnis der Verarbeitungstätigkeiten, Art. 30 (2)
- Vornahme der erforderlichen techn.-org. Maßnahmen (TOMs)
- Meldung von Sicherheitsverstößen an den Verantwortlichen, Art. 33 (2)
- Unterstützung bei der Datenschutzfolgenabschätzung
- Benennung eines Datenschutzbeauftragten

Auftragsdatenverarbeitung Rechtsfolgen

Rechtsfolgen

- Datentransfer zum und Verarbeitung beim Auftragsverarbeiter ist privilegiert, d.h. sie bedarf keiner gesonderten Rechtsgrundlage neben dem Auftrag.

- Geldbußen wegen Verstoß gegen die eigenen Pflichten können gegen den Auftragsverarbeiter direkt verhängt werden.

- Ein fehlender Vertrag über die Auftragsverarbeitung ist für beide Parteien bußgeldbewährt, so dass Auftragnehmer einen solchen aus Eigeninteresse anbieten sollten.
  Hinweis: Der Vertrag lässt sich bei einigen Hosting- und Mailprovidern als PDF herunterladen, unterzeichnen und zur Dokumentation nehmen.

Auftragsdatenverarbeitung Rechtsfolgen

Rechtsfolgen

- Auftragsverarbeiter haftet nur für die Verletzung der speziellen Pflichten eines Auftragnehmers oder bei Verstoß gegen eine Weisung auf Schadensersatz, Art. 82 (2).
  Bei Überschreiten des Auftrags wird Auftragsverarbeiter mit allen Pflichten und Risiken zu einem Verarbeiter.
  - D.h. er hat alle datenschutzrechtlichen Pflichten
  - D.h. nicht, dass die Daten da dann auch zu Recht verarbeitet werden, vielmehr wird regelmäßig eine unzulässige Verarbeitung, ggf. auch ein sanktionsfähiger Verstoß vorliegen.

Auftragsdatenverarbeitung in Drittstaaten

Ist Sitz des Auftragnehmers im Drittstaat möglich?

- Drittstaat = außerhalb des EWR (EU + Island, Liechtenstein und Norwegen), insbesondere USA
- DSGVO: Art. 27 (1) begründet auch für Auftragsverarbeiter die ausdrückliche Pflicht zur Bestellung eines Vertreters in der Union, d.h. implizit dass Auftragsverarbeitung in Drittstaaten nicht per se verboten sein kann.

Besonders zu beachten bei Drittstaaten

- Besondere Risiken der Datenverarbeitung in Drittstaaten sind m.E. entsprechend zu bewerten und schon zu berücksichtigen bei der Auswahl.
- Mögliche Risiken staatlicher Zugriffe auf Daten in Rechenzentren in Drittstaaten aber auch auf den Auftragsverarbeiter mit Sitz in Drittstaaten (und Rechenzentrum in der EU) können dazu führen, dass im Ergebnis der Schutz der Rechte der betroffenen Personen nicht gewährleistet ist, Art. 28 (1).

Datenverarbeitung im Konzern

Übermittlung von Daten im Konzernverbund:

- Das Datenschutzrecht kennt kein „Konzernprivileg"!
- Erwägungsgrund 48 DSGVO:
  Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.
- Im Erwägungsgrund steht keine direkte Erlaubnis im Sinne einer Rechtsgrundlage, sondern nur ein Anhaltspunkt für die Auslegung des Art. 6 (1) (f) DSGVO.
- Eine Abwägung der Interessen ist zwingend durchzuführen.
- Erforderlichkeitsgrundsatz gilt unverändert.

Zusammenfassung: Konzern

- Auftragsverarbeitung durch ein Konzernunternehmen (z.B. konzerneigene Rechenzentrum)
  - Auftragsdatenverarbeiter sind privilegiert bei Rechtsgrundlage für Datentransfer
  - Verantwortlichkeit und Kontrolle im Konzernverbund besonders gut durchsetzbar aber es muss auch eine reale Auswahlmöglichkeit der Verantwortlichen (etwa Konzerntochter) geben, sonst keine wirksame Auftragsverarbeitung möglich.

Transparenz bei Auftragsdatenverarbeitung

- Auftragsverarbeiter bleibt „Empfänger" von Daten.
- Über Empfänger oder Kategorien von Empfängern ist zu informierten, Art. 13 (1) (e) und 14 (1) (e) DSGVO.
- Bei Rückgriff auf eine computer-lesbare Policy ggf. eine automatisierte Verarbeitung sind die Empfänger zu benennen.
  - Ist Empfänger bereits bekannt, muss dieser konkret benannt werden, idealerweise mit Kontaktadresse
  - Kann nur eine Kategorie benannt werden, erfolgt Transparenzwahrung durch den Empfänger
- Eine ideale Nutzeroberfläche würde ermöglichen, nach Daten, Zwecken, Empfängern zu sortieren

TRAPEZE

https://trapeze-project.eu

TOMs zur Sicherstellung der Vertraulichkeit bei Auftragsdatenverarbeitung

- Bereits bei der Auswahl von Auftragsverarbeitern sollte darauf geachtet werden, dass je nach Sensibilität der Daten auch schon ein Zugriff der dortigen Mitarbeiter und Administratoren ausgeschlossen ist.

- Bei herkömmlichen Maßnahmen ist eine verlässliche und regelmäßig per Stichproben kontrollierte Protokollierung Pflicht.

- Ideal sind Systeme, die auch Zugriffe von Administratoren des Auftagnehmers sicher protokollieren oder gar ausschließen

Zusammenfassung

- Sind mehrere an der Datenverarbeitung beteiligt ist deren Verhältnis zueinander zu klären.

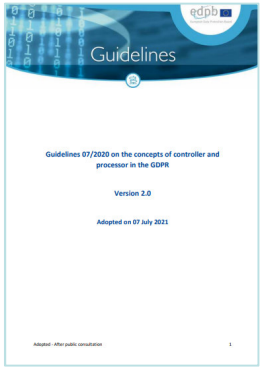
- Gemeinsame Verantwortlichkeit lässt die Notwendigkeit einer RGL nicht entfallen! Das Recht, die Daten zu verarbeiten, muss schon vorher vorhanden sein.

- Anders bei rechtmäßiger Auftragsverarbeitung, die für die Datenflüsse vom Verantwortlichen zum Auftragnehmer die Rechtsgrundlage darstellt und auch den Auftragsverarbeiter in der Haftung besser stellt.

Weiterführendes

- DSK zur gemeinsamen Verantwortlichkeit
  https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_16_Gemeinsame-Verantwortliche.pdf

- Europäischer Datenschutzausschuss
  Guidelines 07/2020 on the concepts of controller and processor in the GDPR
  Version 2.0 Adopted on 07 July 2021
  https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf



- LfD BaWü
  zusammenfassende FAQ zu Guidelines 7/2020 in deutscher Sprache
  https://www.baden-wuerttemberg.datenschutz.de/faq-zur-abgrenzung-der-verantwortlichkeiten-und-des-begriffs-der-auftragsverarbeitung/

Gesundheitsdatenschutz

Recht der Berufsgeheimnisträger

Medizin- und Sozialdatenschutz

1. Geheimnisschutz
2. Gesetzesgrundlagen, Datenerhebung
3. Einwilligung – Schweigepflichtsentbindungserklärung
4. Zweckbindung und Erforderlichkeit
5. Datenübermittlung
6. Betroffenenrechte, insbesondere Akteneinsichtsrechte
7. Datensicherheit
8. Kontrolle

Fragen

- Patientendaten beim Arzt unterliegen einem besonderen Schutz. Welche Gründe könnte es dafür geben? Wer hat ein Interesse an diesem Schutz?

- Welche weiteren Berufsgeheimnisträger kennen sie?

- Welche Sozialversicherungsträger (‚Sozialversicherungen') kennen Sie?

- Welche Gründe kann es geben Daten bei Sozialversicherungsträgern besonders zu schützen?

Gründe für Schweigepflicht und Sozialgeheimnis

Ärztliche Schweigepflicht

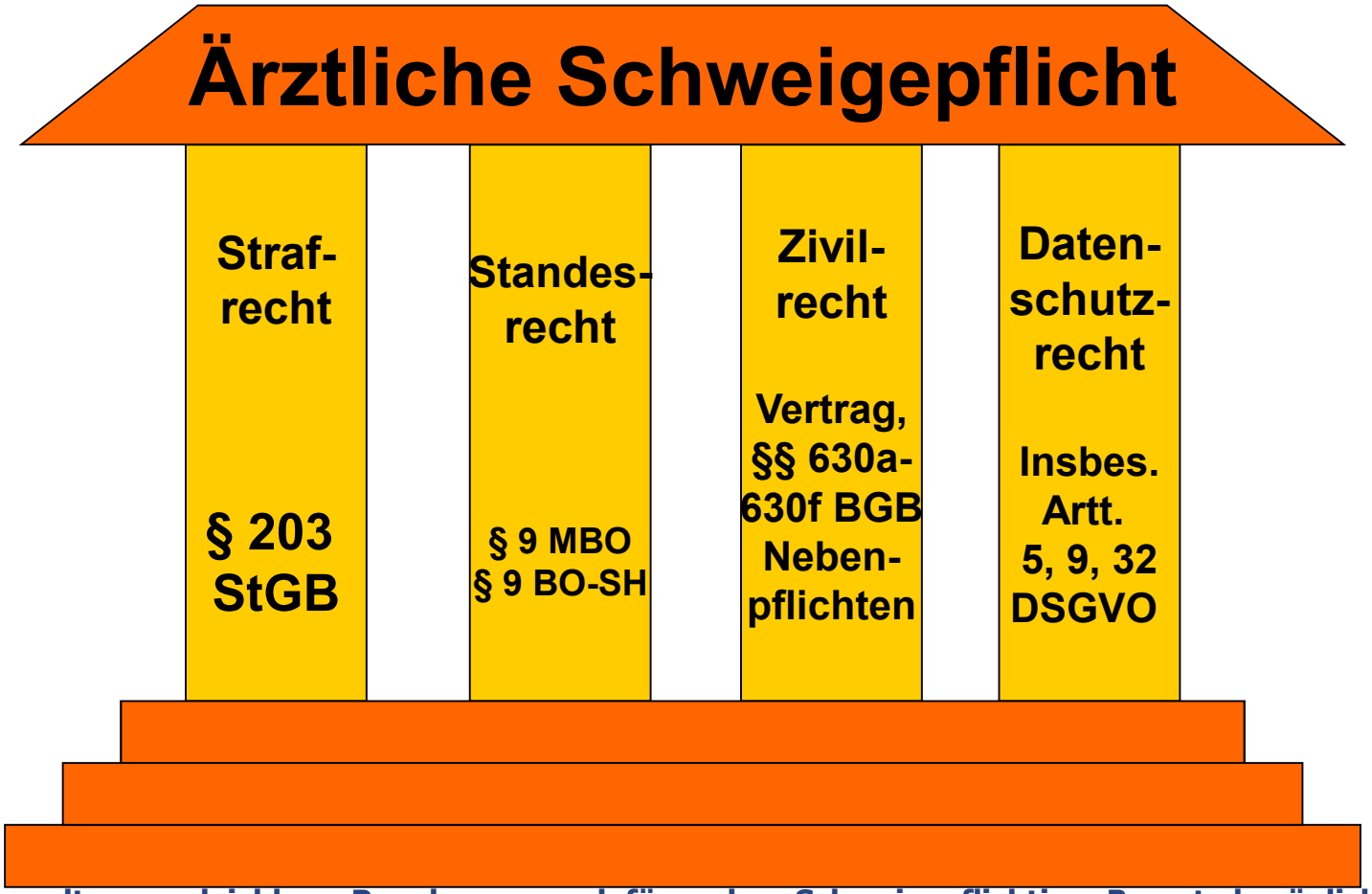
- Persönlichkeitsrecht des Patienten
- staatliches Interesse an gesunden Bürgern und Vertrauen in die Vertraulichkeit der Arzt-Patientenbeziehung
- Eigeninteresse der Ärzte – Vertrauen der Patienten (therapeutisch und wirtschaftlich – siehe Erläuterungen zum Hippokratischen Eid)
- besonders schutzbedürftige Daten

Sozialgeheimnis

- Persönlichkeitsrecht des Betroffenen
- staatliches Interesse an der Vermeidung sozialer Notlagen
- Angehörige einer Sozialversicherung (ob zwangsweise oder freiwillig) sollen nicht mehr staatlichen Eingriffen ausgesetzt sein als andere
- besonders schutzbedürftige Daten (insbes. Gesundheit, Vermögen, soziale Verhältnisse)

Beachte: Auch Datenschutzrechtlich unterliegen Gesundheitsdaten als besondere Arten von Daten nach § 9 DSGVO besonderen datenschutzrechtlichen Anforderungen. Im Sozialrecht finden sich diese im SGB X.

*Grundlagen der ärztlichen Schweigepflicht**



*** im Kern gelten vergleichbare Regelungen auch für andere Schweigepflichtige: Beamte bezüglich Amtsgeheimnissen, Rechtsanwälte, Steuerberater, Ehe-, Familien- oder Suchtberater, Sozialarbeiter, Mitarbeiter bei Krankenkassen… Unterschiede bestehen bezüglich der anwendbaren Rechtsgrundlagen.**

Umfang und Adressatenkreis der ärztlichen Schweigepflicht

§ 203 StGB: Verletzung von Privatgeheimnissen

- Adressatenkreis: u.a. Ärzte, Zahnärzte, Tierärzte, Heilberufe mit staatl. Prüfung, Psychologen, Rechtsanwälte, Notare, Steuerberater, Ehe- Familien- & Jugendberater, Mitglieder von Beratungsstellen, Sozialarbeiter, Mitarbeiter privater Krankenkassen bzw. Unfall- oder Lebensversicherungen
- Umfang: Bereits die Tatsache, dass jemand Patient ist
- „unbefugte" Offenbarung eines fremden Geheimnisses
  - Keine Mitteilung an Familienmitglieder der Patienten
  - Schweigepflicht gilt idR über den Tod des Patienten hinaus
  - Rechtfertigung der Geheimnisoffenbarung durch
    - Einwilligung
    - Mutmaßliche Einwilligung (z.B. bei Bewusstlosen)
    - Gesetzliche Offenbarungspflichten (z.B. § 138 StGB)
    - Rechtfertigender Notstand (z.B. § 34 StGB)

§ 203 StGB Verletzung von Privatgeheimnissen **! spare slide !**

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten,
3a. Organ oder Mitglied eines Organs einer Wirtschaftsprüfungs-, Buchprüfungs- oder einer Berufsausübungsgesellschaft von Steuerberatern und Steuerbevollmächtigten, einer Berufsausübungsgesellschaft von Rechtsanwälten oder europäischen niedergelassenen Rechtsanwälten oder einer Berufsausübungsgesellschaft von Patentanwälten oder niedergelassenen europäischen Patentanwälten im Zusammenhang mit der Beratung und Vertretung der Wirtschaftsprüfungs-, Buchprüfungs- oder Berufsausübungsgesellschaft im Bereich der Wirtschaftsprüfung, Buchprüfung oder Hilfeleistung in Steuersachen oder ihrer rechtsanwaltlichen oder patentanwaltlichen Tätigkeit,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle
anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Amtsträger oder Europäischer Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,
anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.
(2a) (weggefallen)
(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

Rechtliche Bedeutung der Schweigepflicht

- Verfassungsrechtliche Ausgangslage: Dem Bürger ist alles erlaubt, was nicht verboten ist (Art. 2 Abs. 1 GG: Recht auf freie Entfaltung der Persönlichkeit, insb. allgemeine Handlungsfreiheit).
- Im Datenschutz gilt aber auch für Private: Alles ist verboten, was nicht erlaubt ist (Art. 6 (1) und Art. 5 (1) (a) DSGVO). – Jeder Umgang mit personenbezogenen Daten bedarf einer rechtlichen Grundlage. [Stichwort: Rechtmäßigkeit]

- In Bereichen, die einem besonderen Geheimnisschutz unterstellt sind (neben der ärztlichen Schweigepflicht und dem Sozialgeheimnis etwa auch das Steuergeheimnis) werden an die rechtlichen Grundlagen besondere Anforderungen gestellt: Daten dürfen nur dann erhoben, verarbeitet und übermittelt werden, wenn ***bereichsspezifische*** Regelungen dies erlauben.
  Also bei speziellem Verbot braucht es eine spezielle Ausnahme.

Grenzen der Schweigepflicht: Beispiele

- Bankräuber kündigt Tat beim Arzt an: Pflicht zur Anzeige nur bei bestimmten geplanten (künftigen) Straftaten (vgl. § 138 StGB). Im Übrigen gilt Schweigepflicht
- Patient fährt regelmäßig unter Alkoholeinfluss Auto: Mitteilung an Register oder Führerscheinbehörde möglich / geboten / Pflicht? § 34 StGB
- Einschaltung externer Inkassounternehmen bei der Behandlungsabrechnung als Auftragsverarbeiter denkbar (siehe unten)
- HIV-Patient beim Arzt: Mitteilung der HIV-Infektion an den/die Sexualpartner(in)? § 34 StGB bei Anhaltspunkten für eine *konkrete* Ansteckungsgefahr vertretbar. Ggf. jetzt anders denkbar bei Virostatika (OLG Frankfurt sah Pflicht(!) zur Warnung bei erklärter Absicht des Patienten zu ungeschütztem Geschlechtsverkehr mit einer bestimmten Person, die ebenfalls Patient desselben Arztes war. Sehr umstr. Urteil)
- Arzthaftungsprozess: Mitteilung von Patientendaten zur rechtlichen Verteidigung? Nach § 34 StGB zulässig, aber nur im erforderlichen Umfang
- Polizei fahndet nach einem Bankräuber und befragt den Arztpraxen, ob dieser dort in Behandlung war: Schweigepflicht

§ 138 StGB Nichtanzeige geplanter Straftaten **! spare slide !**

(1) Wer von dem Vorhaben oder der Ausführung
1. (weggefallen)

2. eines Hochverrats in den Fällen der §§ 81 bis 83 Abs. 1,

3. eines Landesverrats oder einer Gefährdung der äußeren Sicherheit in den Fällen der §§ 94 bis 96, 97a oder 100,

4. einer Geld- oder Wertpapierfälschung in den Fällen der §§ 146, 151, 152 oder einer Fälschung von Zahlungskarten mit Garantiefunktion in den Fällen des § 152b Abs. 1 bis 3,

5. eines Mordes (§ 211) oder Totschlags (§ 212) oder eines Völkermordes (§ 6 des Völkerstrafgesetzbuches) oder eines Verbrechens gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches) oder eines Kriegsverbrechens (§§ 8, 9, 10, 11 oder 12 des Völkerstrafgesetzbuches) oder eines Verbrechens der Aggression (§ 13 des Völkerstrafgesetzbuches),

6. einer Straftat gegen die persönliche Freiheit in den Fällen des § 232 Absatz 3 Satz 2, des § 232a Absatz 3, 4 oder 5, des § 232b Absatz 3 oder 4, des § 233a Absatz 3 oder 4, jeweils soweit es sich um Verbrechen handelt, der §§ 234, 234a, 239a oder 239b,

7. eines Raubes oder einer räuberischen Erpressung (§§ 249 bis 251 oder 255) oder

8. einer gemeingefährlichen Straftat in den Fällen der §§ 306 bis 306c oder 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 4, des § 309 Abs. 1 bis 5, der §§ 310, 313, 314 oder 315 Abs. 3, des § 315b Abs. 3 oder der §§ 316a oder 316c
zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterläßt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer
1. von der Ausführung einer Straftat nach § 89a oder
2. von dem Vorhaben oder der Ausführung einer Straftat nach § 129a, auch in Verbindung mit § 129b Abs. 1 Satz 1 und 2,
zu einer Zeit, zu der die Ausführung noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde unverzüglich Anzeige zu erstatten. § 129b Abs. 1 Satz 3 bis 5 gilt im Fall der Nummer 2 entsprechend.

(3) Wer die Anzeige leichtfertig unterläßt, obwohl er von dem Vorhaben oder der Ausführung der rechtswidrigen Tat glaubhaft erfahren hat, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Schweigepflicht Sonderregelungen

Es gibt Spezialgesetzliche Sonderregelungen etwa

- Für Meldungen zum Krebsregister
- Meldung einer Kindeswohlgefährdung[1] durch Mediziner, Psychologen, Familienberatung, Sozialarbeiter, Lehrkräfte in abgestuftem Vorgehen § 4 KKG[2]:
  - Erörterung der Situation mit Kind oder Sorgeberechtigten und auf Inanspruchnahme von Hilfe hinwirken
  - Rücksprachemöglichkeit und Beratung durch die Jugendhilfe für die Normadressaten (Ärzte,…) zur Beurteilung der Kindeswohlgefährdung mit Einbeziehung von Kind / Eltern
  - Gestattung, das Jugendamt einzuschalten (keine Pflicht)

  => „Datenschutz verhindert keinen Kinderschutz!“

[1] KKG: Gesetz zur Kooperation und Information im Kinderschutz

[2] Dazu TB 2019 des ULD: https://www.datenschutzzentrum.de/tb/tb37/kap04_5.html#451

Sozialgeheimnis

- § 35 Abs. 1 Satz 1 SGB I – Sozialgeheimnis:
- Berechtigter: „Jeder" (über den Sozialdaten erhoben werden) Leistungsempfänger, Vermieter, Arbeitgeber,...
- Adressat: alle Leistungsträger (nicht Leistungserbringer wie z.B. Ärzte)

  => Institutionenbezogenes Spezialrecht für Leistungsträger
- Klarstellung: Auch innerhalb eines Leistungsträgers dürfen Daten nur Befugten zugänglich sein, § 35 I SGB I

- Gegenstand: Sozialdaten nach § 67 Abs. 1 SGB X

  „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener)"
- Normbefehl:
  - Verbot „unbefugter" Datenverarbeitung
  - § 35 II SGB I: nur nach den Voraussetzungen der §§ 67 ff. SGB X

Erhebung von Sozialdaten, § 67a SGB X

- Grundsatz: Sozialdaten dürfen erhoben werden, wenn sie zur Aufgabenerfüllung erforderlich sind
  - Keine Datenerhebung auf Vorrat
  - Nur entscheidungserhebliche Tatsachen
  - Daten müssen auch tatsächlich Verwendung finden
  - Kontoauszüge: Vorlagepflicht für Auszüge der vergangenen 3 Monate, Schwärzung bei bes. Arten personenbezogenen Daten statthaft. § 67a I 2, i.V.m. § 67 XII SGB X

Zu Kontoauszügen siehe: BSG, Urteil vom 19. 9. 2008 - B 14 AS 45/ 07 R ; und unter: https://www.datenschutzzentrum.de/artikel/1109-.html (Stand 2017)

Erhebung von Sozialdaten, § 67a SGB X

- Es gilt der Grundsatz der Datenerhebung beim Betroffenen

- Transparenz: Betroffener muss bei Erhebung über den Zweck der Erhebung und Verarbeitung, die verantwortliche Stelle und die relevanten Rechtsvorschriften informiert werden.

- Hinweis auf Rechtsfolgen: Soweit eine Auskunftspflicht besteht oder bei Nichtauskunft Nachteile drohen, ist darauf hinzuweisen.
  (Auskunftspflicht z.B. in § 60 SGB I, Folgen § 66 SGB I)

Einwilligung in eine medizinische Untersuchung

Medizinrechtliche Einwilligung

- Einwilligung in den Eingriff, andernfalls ist Behandlung eine Körperverletzung
- Informed consent = Aufklärung und freie Einwilligung
- Aufklärung über
  - 1. Diagnose und Diagnosesicherheit
  - 2. Verlaufsprognose
  - 3. Wesen der Maßnahme, Mitwirkungspflichten
  - 4. Erfolgsquote, Nutzen
  - 5. Komplikationen und Komplikationswahrscheinlichkeit
  - 6. Handlungsalternativen
  - 7. Wirtschaftliche Aufklärung
- Schwerpunkt: Einwilligung in körperlichen Eingriff
- Aber auch: Einwilligung in Informationsgewinnung und übermittlung (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen)

-

Datenschutzrechtliche Einwilligung:

- Informierte Einwilligung, Art. 13 DSGVO
- Anforderungen nach Art. 7 DSGVO, insb.:
  - freie Entscheidung, Art. 7 (4)
  - Aufklärung über den Zweck der Datenerhebung oder -verarbeitung Art. 13 (1) (c)
  - Keine Formpflicht aber Nachweisobliegenheit, Art. 7 (1)
  - ggf. besondere Hervorhebung der datenschutzrechtlichen Einwilligungserklärung Art. 7 (2)
  - ausdrücklicher Hinweis auf die Verwendung von Gesundheitsdaten, Art. 8 (2) (a) DSGVO
- Schwerpunkt: Schutz des Rechts auf informationelle Selbstbestimmung
- beachte z.B. § 9 Abs. 3 MBO: Hinweis auf die Daten, die aufgrund einer vermuteten Einwilligung übermittelt werden dürfen

Einwilligung - Beispielsfälle

- Heimlicher HIV-Test – unzulässig, da keine zu erwartende Routineuntersuchung.

- Forschung: Forschung mit anonymisierten Daten ist zulässig, Untersuchungen an personenbezogenen Proben ohne Einwilligung sind i.d.R. unzulässig (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen).
  Aber: Anonymisierung ist zunehmend schwieriger.

- Betriebsarzt: Proband muss über die Untersuchung im Vorwege aufgeklärt werden, insbesondere wenn Untersuchung nicht üblich oder erkennbare Voraussetzung für die angestrebte Tätigkeit ist.

Zweckbindung und Erforderlichkeit

- Der Zweck der Erhebung und Verarbeitung muss hinreichend bestimmt sein. Rahmen ist in der Regel das konkrete Behandlungsverhältnis
- Der Umfang der Erhebung und Verarbeitung der Daten muss erforderlich sein. (Die Erforderlichkeit wird häufig durch die gesetzgeberische Wertung sichergestellt. In diesem Fall ist sie nur gesondert zu prüfen, wenn ausdrücklich gefordert, z.B. § 27 Abs. 1 BDSG nF. für Forschung mit Daten)
- Arzthaftungsprozess: Es dürfen nur Patientendaten dem RA offengelegt werden, deren Kenntnis für den Prozess erforderlich ist, Art. 9 (2) (f) DSGVO. Schwierige Bestimmung der Erforderlichkeit, weil Vor- oder Miterkrankungen u.a. für die Bestimmung der Schadenshöhe relevant sind und diese Bewertung oft nur im Dialog mit dem RA erfolgen kann.
- Forschung, Archive, Statistik: Art. 9 (2) (j) DSGVO i.V.m. nationalen Gesetzen wie § 27 BDSG-neu, §§ 13, 26 LDSG-SH

Typische Übermittlungsbefugnisse

- Abrechnung mit der Kassenärztlichen Vereinigung
- Bei Privatliquidation ist bisher Einwilligung für Übermittlung an eine Einzugsstelle notwendig – Transparenzpflicht bleibt aber!
  StGB ist kein Hindernis, § 203 III 2 StGB (2017)
- §§ 284 ff, 294 ff SGB V (Vertragsarztrecht)
  - Wirtschaftlichkeitsprüfungen
  - Qualitätsprüfungen z.B. Sonografie (Stichproben)
- Meldepflichten: InfektionsschutzG, KrebsregisterG
- Bei vor-, mit und nachbehandelnden Ärzten wird konkludente Einwilligung unterstellt - d.h. Widerspruch ist möglich, § 9 MBO
- Praxisinterne Übermittlung, gegenseitige Einsicht in Patientenakten:
  (+) Gemeinschaftspraxis (Partner, Gesellschaft), MVZ,
  (-) Praxisgemeinschaft (gemeinsam genutzte Räume und Mitarbeiter), angegliederte Kosmetikerin beim Dermatologen
- Kliniken: Meldeschein zur Einsicht der Polizei, wie bei Hotel

Auftragsverarbeitung

- Bis 2017 war Auftragsverarbeitung für Berufsgeheimnisträger nur in Ausnahmefällen (Ländergesetze) möglich oder auf Grund einer Einwilligung.
- Seit 2017: § 203 Abs. 3 StGB:

  Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

- Damit entfällt die Strafbarkeit
- Das ist für sich allein aber keine Erlaubnis.
- Als Rechtsgrundlage kommt dann eine Auftragsverarbeitung nach der DSGVO in Betracht.
- Pflicht: dem Risiko angemessene tech.-org. Maßnahmen

Auftragsverarbeitung

- Besondere Anforderungen an die Auftragsverarbeitung im Gesundheitsbereich:
  - Bekanntgabe der Identitäten der Auftragsverarbeiter, Zwecke, Umfang der Verarbeitung vor Beginn der Behandlung.
  - Besonders sorgfältige Auswahl aller Auftragsverarbeiter.
  - Klare Verpflichtung auf die Verschwiegenheit zwingend – Auftragnehmer muss alle eingesetzten Mitarbeiter verpflichten.
  - Soweit möglich sollen Betroffene einzelnen Verarbeitungen widersprechen können – Praktisch nicht möglich beim Haupt-IT-Dienstleister eine Klinik, denkbar aber durchaus bei der Auswahl eines externen Medizin- oder Dentallabors.

Übermittlung von Sozialdaten, §§ 67d ff SGB X

- Übermittlung Grundsatz: Es bedarf einer **gesonderten Übermittlungsbefugnis**, die von der übermittelnden Stelle zu prüfen ist. Soweit eine andere Stelle anfragt, trägt diese die Verantwortung für die Richtigkeit der Anfrage, §_67d II SGB X

- diverse Übermittlungsbefugnisse in §§ 68-77 SGB X und anderen Sonderregelungen, z.B. für den Datenabgleich gegen Sozialleistungsmissbrauch und Schwarzarbeit

- Bei erhobenen medizinischen Daten Weitergabe nur, wenn sie dem Arzt selbst gestattet gewesen wäre, § 76 I SGB X

Betroffenenrechte im Medizinbereich

<u>medizinrechtliche Ansprüche</u>

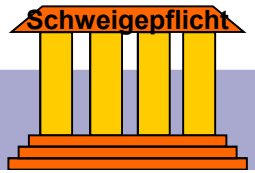
- Medizinrechtlicher Auskunftsanspruch aus Art. 2 I i.V.m. Art. 1 I GG
  - Patientenautonomie als Ausprägung des Rechts auf freie Entfaltung der Persönlichkeit
- Einsicht in Patientenakte:
  - § 630g BGB als Teil des Behandlungsvertrags
  - § 10 II Berufsordnung Ärzte
- Alle objektive Befunde unterliegen dem Einsichtsrecht. Arzt darf aber persönliche Notizen schwärzen.

<u>datenschutzrechtliche Ansprüche</u>

- Art. 13, 14 DSGVO Benachrichtigung
- Art. 15 DSGVO Auskunft
- Art. 17 DSGVO Löschung
- Art. 18 DSGVO Sperrung

- Zusätzlich: Schadensersatzanspruch

Für den Sozialdatenschutz finden sich entsprechende Regelungen in den §§ 84 ff. SGB X

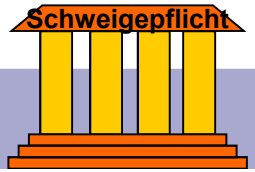


Datensicherheit im Gesundheitsbereich

- Gesundheitsdaten sind besondere Arten von Daten und unterliegen je nach datenverarbeitender Stelle besonderer Berufsgeheimnisse.
- Es sind die **geeigneten** Maßnahmen zu treffen mit Rücksicht u.a. auf das **Risiko für die Betroffenen**.
- Umfang hängt von Quantität und Qualität der Daten ab, insbesondere welche Einschnitte Betroffene bei einem Datenverlust erleiden würden.
- Arzt hat dabei sicherzustellen:
  - Vertraulichkeit — Keine Einsicht durch Dritte
  - Verfügbarkeit — Dokumentation, Folgebehandlungen
  - Integrität — Aufbewahrungsfirsten

Kontrolle im Gesundheitsbereich

- Interne Kontrolle erfolgt durch betrieblichen / behördlichen Datenschutzbeauftragten.
- Externe Kontrolle je nach rechtlicher „Säule“
  - DSGVO: Datenschutzbehörden
  - Berufsrecht: Kammern (Ärztekammer, Anwaltskammer, Notarkammer, etc.)
  - Strafrecht: Staatsanwaltschaft. Wenn ein solcher Fall beiden Aufsichtsbehörden landet, wird er an die zuständige StA abgegeben. Da § 203 StGB ein Antragsdelikt ist, muss ein Geschädigter Strafantrag stellen, § 205 StGB.
  - BGB: Patient verfolgt seine Ansprüche selbst auf dem Zivilrechtsweg.



Aus den Forschungsprojekten

Gestern war Fließtext. Übersichtliche, verständliche und nachvollziehbare Darstellung von Datenverarbeitungs-Vorgängen hilft bei der Transparenz und bei Akzeptanz.

- Art. 21 (5) Widerspruch per automatisierter Verfahren unter Verwendung technischer Spezifikationen
- Art. 10 (1b) ePrivacy-VO (Parlamentsentwurf)
  Unbeschadet des Absatzes 1 kann, sofern der Datenschutzausschuss eine bestimmte Technologie zugelassen hat, für die Zwecke des Artikels 8 Absatz 1 Buchstabe b die Einwilligung jederzeit – sowohl in der Endeinrichtung als auch mittels von dem bestimmten Dienst der Informationsgesellschaft bereitgestellter Verfahren – erteilt oder widerrufen werden.

SPECIAL

TRAPEZE

https://trapeze-project.eu

Herzlichen Dank für die gemeinsame Diskussion zum Thema

Harald Zwingelberg
vorlesung@zwingelberg.de
0431 / 988-1222 (dienstl.)

www.datenschutzzentrum.de/projekte

PANELFIT

AnoMed

TRAPEZE

EMPRI-DEVOPS

SPECIAL

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug