Institut für Informationsrecht

Neue rechtliche Anforderungen an Medical Apps & Medical Software

Prof. Dr. Thomas Wilmer

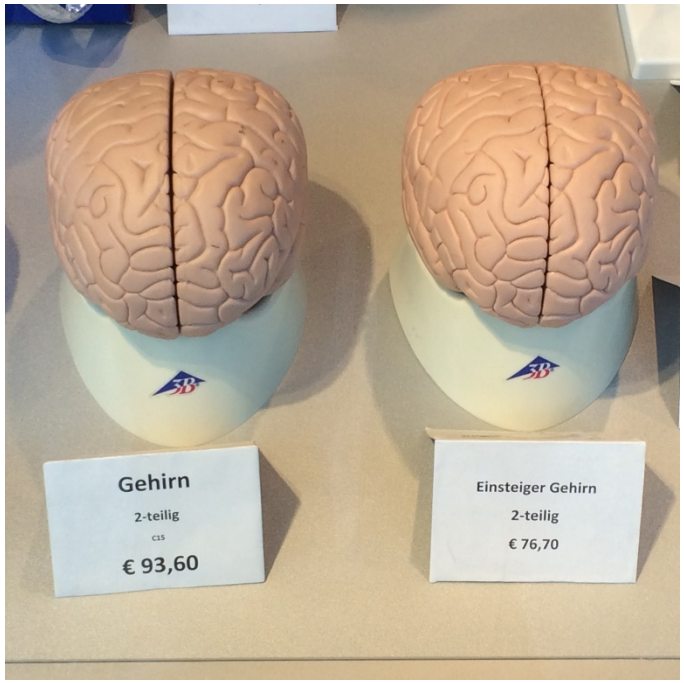
Rechtsrahmen: IoT, Big Data, vernetzte Medical Device |Haftung
Datenschutz-Grundverordnung | Decision Support Systeme

LISAvienna Business Treff 07.11.2017

Übersicht

A. IoT, Big Data, Medical Device, Decision Support:
   Chancen und Risiken autonomer und vernetzter Systeme
B. Compliance, Einfluss des Softwarerechts: Rechte sichern
C. Datenschutz: Grundlagen, Medizinbereich und DSGVO

A. IoT, Big Data, Medical Device, Decision Support: Chancen und Risiken autonomer und vernetzter Systeme; Medizin 4.0



Institut für Informationsrecht

Was ist neu an smarter Medizin?

Früher:

- Querulant
- Fleischbällchen
- Entscheidungsschwach sein
- Erwartbarer Verlauf
- Deutscher Investor
- Zu viel Elektronik

Jetzt:

- Customer
- Meatballs
- Being Open Minded
- Worst Case
- Kraut Funding
- Smart Product

Automatisierte Systeme: Gewährleistung und Haftung

1. Big Data und vernetzte Systeme, „health cloud“:

Besondere Chance:

Datenaggregation

Besondere Probleme:

Datenaggregation und Verantwortungszuordnung

Automatisierte Systeme: Gewährleistung und Haftung

2. IoT

Besondere Chance:

Flexibilität und Ubiquität

Besondere Probleme:

Verantwortungszuordnung

Automatisierte Systeme: Gewährleistung und Haftung

3. Medical Support Systems

Besondere Chance:

Flexibilität

Besondere Probleme:

Verantwortungszuordnung und Haftung

Automatisierte Systeme: Gewährleistung und Haftung

Beispiele

„Bitkom Innovators' Pitch“

Ovula Ring: Eisprungerkennung mit 99% Sicherheit

Kombination aus Implantat und App

Automatisierte Systeme: Gewährleistung und Haftung

„Bitkom Innovators' Pitch": Medexo

Trends bei smarter Medizin

Erweiterung Smart Hospital…
Überwachung Demenzkranker

•Erfassung von

- Herzfrequenz
- Atmung
- Position im Gebäude
- Bewegung
- Körperhaltung

•durch Sensoren in den Wänden, Kameras, implantierte Chips.

•Smart Metering auch für Menschen…?

Trends bei smarter Medizin

Smart Home Hospital…Überwachung Demenzkranker zu Hause

https://www.bka.gv.at/DocView.axd?CobId=32306:

Vorschlag für ein System, das über mehrere Sensoren, die sowohl am Körper getragen werden als auch im Haus (bei der Eingangstüre) und in verschiedenen Gegenständen wie Schuhen, Schlüsselbund, Brillen oder Gürteln angebracht sind, die Position einer Person überwachen kann. Verschiedene Situationen wie das Verlassen des Hauses können identifiziert werden, und Betreuungspersonen können informiert werden. Schließlich gibt es Technologien, die der mentalen Aktivierung der PatientInnen dienen. Denkbar wäre daneben ein interaktives Unterhaltungssystem, das sie über Virtual Reality in einer sicheren und risikofreien Umgebung Situationen erleben lässt, die sie aus ihrem früheren Leben kennen.

Grenzen smarte Medizin und Lifestyle

Smart Clothing

„Self Tracking, Quantified Self“

VITALDATEN-MONITORING

Tragbare Elektroden, kombiniert mit moderner Informationstechnologie die das Monitoring von Vitaldaten im alltäglichen Leben ermöglichen – ohne den Komfort zu beeinträchtigen. Mit der Bluetooth Anbindung an das Smartphone oder beispielsweise Tablet-Geräte ist der BioMan perfekt für die Gewichtskontrolle, Training und Gesundheitsmonitoring.

http://de.aiqsmartclothing.com/

Fallbeispiel zur Diskussion

Ein Hersteller „Hormon 4.0“ möchte eine App anbieten, die in Kombination mit einem implantierten Sensor und einer implantierten Pumpe bestimmte Hormonausschüttungen im Patienten bei besonderen Erkrankungen regelt. Es soll auch erfasst werden, welche – über das Smartphone erhobene – Lebensumstände den Gesundheitsstatus beeinflussen.

Der Hersteller möchte diese Daten nutzen, um weitere Produkte zu entwerfen, er möchte die Daten aber auch separat veräußern können.

Zugleich möchte er keine Haftungsfälle riskieren…

Automatisierte Systeme: Gewährleistung und Haftung

Definition automatisierter Systeme in der Medizin

- **Bestandsaufnahme der Entwicklung**
  - Rechtliche Einordnung
  - Konsequenzen für Einkauf und Vertragsgestaltung

• Definition automatisierte Systeme

- **Selbstständiger Ablauf eines komplexeren Prozesses**
- **Begrenzte Möglichkeit sofortigen Eingriffs**
- **Umfangreiche Vorarbeiten notwendig**
  - **Direkte oder indirekte Steuerung**
  - **Produktion**
  - **Automotive, Automated Systems**
    - **Körperinterne Pumpen, Schrittmacher**
    - **Sonstige**

- **Definition automatisierte Systeme**

  - **Grundentscheidung beim Einsatz von Medical Devices:**

  - **Grad der Automatisierung:**

    Direkte oder indirekte Steuerung?

Automatisierte Systeme: Gewährleistung und Haftung

Verdeckte Fehlfunktion bei direkter Steuerung:

Profi-Kopierer verdreht Zahlen: Folgen für Medikamentengabe?

http://www.spiegel.de/netzwelt/apps/blogger-schreibt-bug-xerox-scankopierern-sollen-zahlen-vertauschen-a-914897.html

„Aus 14 wird 17, aus 21 manchmal 14: Ein Informatiker hat einen kuriosen Fehler bei Xerox-Kopierern beobachtet - offenbar vertauscht die Gerätesoftware beim Kopieren Zahlen. Xerox prüft den Fall.

Auf dem Tisch liegt ein Medikamentenplan. An einem Wochentag sind die Daten jedoch anders an allen anderen: Man denkt, jemand hat sich vertippt oder etwas vertauscht. Doch den Fehler, den ein Informatiker beschreibt, hat kein Arzt, sondern ein Kopierer begangen. Das Original-Dokument ist korrekt beschriftet, erst auf der Kopie hat das Gerät die Zahlen für die Medikamentengabe vertauscht.

Automatisierte Systeme: Gewährleistung und Haftung

Verdeckte Fehlfunktion bei direkter Steuerung: Profi-Kopierer verdreht Zahlen

http://www.spiegel.de/netzwelt/apps/blogger-schreibt-bug-xerox-scankopierern-sollen-zahlen-vertauschen-a-914897.html

„Der Informatiker David Kreisel berichtet in seinem Blog, dass er einen Software-Fehler in den Kopierern des Unternehmens Xerox gefunden hat. Detailliert beschreibt er eine kleine Versuchsreihe und wie er auf das Problem aufmerksam gemacht wurde. Der reproduzierbare Fehler trete wohl bei Zahlen auf, die in einer gerade noch lesbaren Auflösung auf Dokumenten abgedruckt sind. Sie werden bei Kopien durch andere Zahlen aus demselben Dokument ersetzt.“

Automatisierte Systeme: Gewährleistung und Haftung

Verdeckte Fehlfunktion bei direkter Steuerung: Profi-Kopierer verdreht Zahlen

„Xerox prüft den Fall derzeit, äußert sich aber nicht öffentlich.

Sollte der Fehler tatsächlich bei mehrere Xerox-Drucker auftreten, könnte das erhebliche Probleme mit sich bringen.

(...)

Als in seiner Versuchsreihe getesteten Geräte nennt der Informatiker Kreisel die Scankopierer der Xerox-WorkCentre-Reihe, darunter Xerox WorkCentre 7535 und 7556. Auf Ihnen konnte er den Fehler in wechselnder Häufigkeit reproduzieren. Auch die neueste Software-Version behebt das Problem derzeit noch nicht.“

Automatisierte Systeme: Gewährleistung und Haftung

Fehlfunktion bei medizinischen Systemen

Wer trifft die medizinischen Entscheidungen?

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung

Rechtliche Rahmenbedingungen

Öffentliches Recht

- **Geräte- und Produktsicherheitsgesetz (GPSG), ggf. spezifische Bereiche wie**
  - MedizinprodukteG,
  - MDR,
  - Bereichsspezifische Verordnungen

- DSDS (später…)

Automatisierte Systeme: Rechtliche Kriterien der Einordnung

Rechtliche Rahmenbedingungen nach Hilgendorf:

1. Grundlagenfragen: Was bedeuten Konzepte wie „Handlung“, „Zurechnung“ oder „Schuld“ im Zeitalter autonomer Maschinen?
2. Strafrechtliche Haftung
3. Zivilrechtliche Haftung
4. Rechtsfragen der Zulassung
5. Versicherung
6. Arbeitsschutz
7. Datenschutz

Hauptproblem: Vorverlagerung der Verantwortung…Medizinische Kompetenz im Vorfeld

Automatisierte Systeme: Rechtliche Kriterien der Einordnung

Rechtliche Rahmenbedingungen

Risikogruppen / Schadensfälle

- **Personen- und Sachschäden?**
- **Aufzeichnung personenbezogener Daten zur Steuerung?**
- **Nichtzulassung von Systemen?**

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Gewährleistung

Zivilrecht / Vertragsrecht

Mangelbegriff im Vertragsrecht: Der Sollzustand

- **Abhängigkeit von**
  - Drohender Gefahr bei Fehlfunktionen
  - Klarer Definition des beabsichtigten Einsatzes
  - Erhöhte Anforderungen an Robotik gegenüber menschlichen Fehlerraten?

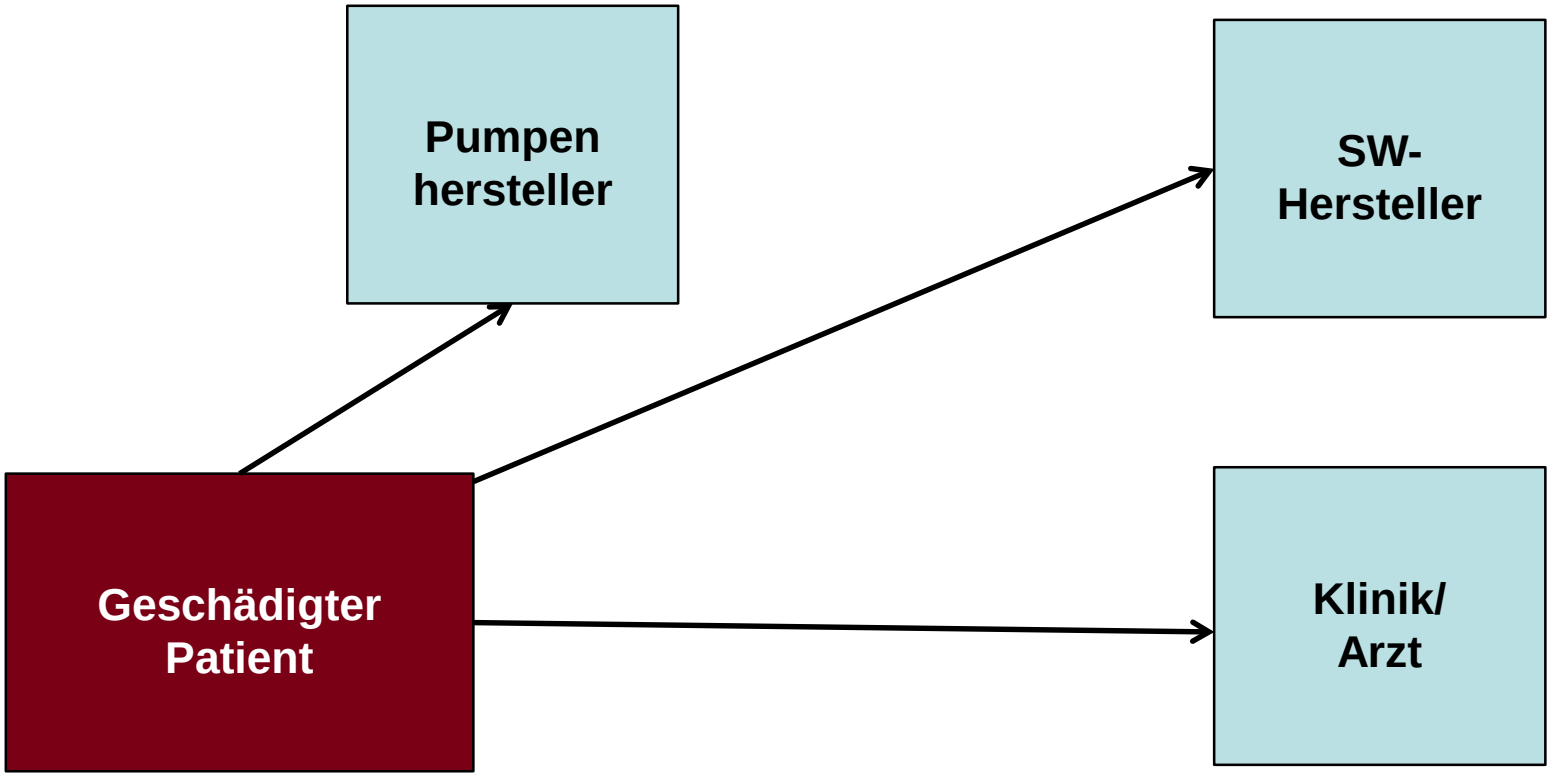
Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungssubjekte

Hardware-hersteller	Software-hersteller	Betreiber (Krankenhaus)	Arzt / Pfleger	System selbst („electronic person“)

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Haftung

- Mögliche Haftende: Die Medikamentenpumpe



Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungssubjekte: Zuordnung des BMWI

- **Betreiber: Eine juristische oder natürliche Person, die das autonome System betreibt bzw. Leistungen damit anbietet.**
- **Systemintegrator: Dies ist das Unternehmen (oder ggf. die Forschungseinrichtung) und seine Handelnden, das das autonome Gesamtsystem einem Betreiber zur Verfügung stellt.**
- **Komponentenhersteller: Dabei handelt es sich um solche Unternehmen, die Bauteile oder Baugruppen für ein autonomes System zuliefern..**

Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungssubjekte: Zuordnung des BMWI

- **Nichtkooperativer Dritter: Dabei handelt es sich um nichteingewiesene Personen mit geringer Einsichtsfähigkeit, bei denen mit unkooperativem Verhalten gerechnet werden muss.**
- **Kooperativer Dritter: Dabei handelt es sich um nichteingewiesene Personen mit erheblicher Einsichtsfähigkeit, bei denen mit unkooperativem Verhalten (wider den gesunden Menschenverstand) nicht gerechnet werden muss.**
- **Werker: Das sind alle Personen, die eine wie auch immer geartete Sicherheitsunterweisung zum Umgang mit autonomen Systemen erhalten haben und mit diesen im Rahmen ihrer Berufstätigkeit interagieren.**

Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungskriterien: Überblick

- **Festlegung des Maßstabs der Sorgfaltspflicht**
  - **Schaffung von Gefährdungslagen**
  - **Menschliche „Perfektion“?**
- **Festlegung von Mitverschuldensmaßstäben**
- **Ausreichende Regelung?**
- **Explizite Gefährdungshaftung de lege lata notwendig (Haftung des Robotik-Halters?)?**

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungskriterien

- **Festlegung des Sorgfaltsmaßstabs**
- **Berechtigte Sicherheitserwartungen des Verkehrs und der zumutbare Aufwand: Welche Bedrohung von Rechtsgütern Dritter besteht, wie hochrangig sind die bedrohten Rechtsgüter sind.**
- **Aber im Bereich der Produkthaftung für Hersteller (von IT-Produkten):**
  - **individuelle besondere Sicherheitserwartungen oder Schadensanfälligkeiten sind nicht zwingend zu berücksichtigen**
  - **Produkte, deren Gefahren jedermann bekannt sind, müssen nicht gegen Missbrauch gesichert werden; auch vor deren Fehlgebrauch muss nicht gewarnt werden.**
  - **Die Pflichten des Produzenten, insbesondere zur Instruktion und Warnung, werden weiter eingeschränkt, wenn die Abnehmer selbst fachkundigen Kreisen angehören und daher weitestgehend selbst die Gefahren des Produktes beurteilen können**

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungskriterien

- **Festlegung des Maßstabs § 1279 ABGB**

  - Es wird aber auch vermuthet, daß jeder welcher den Verstandesgebrauch besitzt, eines solchen Grades des Fleißes und der Aufmerksamkeit fähig sey, welcher bey gewöhnlichen Fähigkeiten angewendet werden kann. Wer bey Handlungen, woraus eine Verkürzung der Rechte eines Anderen entsteht, diesen Grad des Fleißes oder der Aufmerksamkeit unterläßt, macht sich eines Versehens schuldig.

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungskriterien

- **Festlegung des Maßstabs § 1279 ABGB**
  - Konkretisierung der geschuldeten Verkehrspflichten:
    - Stand von Technik und Wissenschaft hinsichtlich der Sicherheit des Produktes. Maßgeblich sind die Erkenntnisse, die zum Zeitpunkt der erforderlichen Gefahrenabwehr verfügbar;
    - öffentlichrechtliche Vorschriften wie DIN-Normen als Anhaltspunkt;
    - Es sei denn, es gibt erkennbare Zusatzgefahren durch das Erzeugnis…

  -> Bei autonomen Systemen?

Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungskriterien

- Der Beherrscher der Gefahrenquelle muss auch für Schäden einstehen, die erst durch das vorsätzliche Ausnutzen der durch das Produkt entstandenen latenten Gefahr durch Dritte entstehen…

Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

- **Mißbrauch mitdenken!**
- **Entsprechend aufklären!**

- **Fanatsie ist gefragt für Begriffe wie ‚vernünftigerweise vorhersehbarer Missbrauch' (‚reasonable foreseeable misuse'), ‚anormaler Gebrauch' (‚abnormal use'), ‚korrekter Gebrauch' (‚correct use') und ‚bestimmungsgemäßer Gebrauch' ('normal use') (ISO 14971 und IEC 62366-1).**

Automatisierte Systeme: Rechtliche Kriterien der Einordnung: Haftung

Mögliche Haftungskriterien

- **Mitverschulden**
  - Anforderungen an die Verkehrspflicht stehen in einem engen Verhältnis zu den dem Dritten abzuverlangenden Bemühungen an vernünftigem Eigenschutz.
  - Nicht gegen jedes Risiko kann Schutz verlangt werden, wenn der Dritte einfacher und mit geringerem Aufwand eine Schädigung als der Pflichtige vermeiden
  - Die Prüfung muss eindeutig ergeben, dass der Dritte ohne großen Aufwand die Verletzung vollständig vermeiden kann,
  - während dem Pflichtigen selbst mit hohen Kosten die vollständige Gefahrenbeherrschung nicht möglich ist.
- **Aufklärung ist essentiell!**

Mögliche Haftungskriterien

Produzentenhaftung

Erfüllung der Verkehrs- und Organisationspflichten bei

- **Konstruktion,**
- **Fabrikation,**
- **Instruktion und**
- **Beobachtung des Produktes**

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Datensicherheit

Institut für Informationsrecht

http://www.t-online.de/computer/sicherheit/id_60595676/forscher-hacken-herzschrittmacher.html

Forscher hacken Herzschrittmacher

25.10.2012, 15:43 Uhr | t-online.de

Barnaby Jack, Sicherheitsexperte der Firma IOActive, hat die kabellose Attacke auf der Sicherheitskonferenz Breakpoint in Australien demonstriert. Sie funktioniert drahtlos auf zehn Meter Distanz, wie das *SC Magazine* berichtet. Der Experte bediente sich dazu der Hardware, mit der Herzschrittmacher eigentlich von Fachpersonal per Funk gewartet und eingestellt werden können. Jack entdeckte in diesem Transmitter eine Sicherheitslücke, über die Angreifer die Programmierung manipulieren können.

Hack nutzt eine sinnvolle Funktion aus

Möglich ist das durch die Defibrillator-Funktion von Herzschrittmachern. Wenn ein Herz schwere Herzrhythmusstörungen hat, kann ein exakt dosierter Elektroschock diese Störung beheben und den normalen Herzschlag wieder herstellen. Genau diese Funktion könnten Angreifer manipulieren und einen maximalen Stromstoß auslösen, der den Träger des Herzschrittmachers tötet.

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Haftung

Problem der Dateninhaberschaft

- ***Patient als Inhaber?***
- ***Arzt als Inhaber?***
- ***Klinik?***
- ***Hersteller?***
- ***Zulieferer?***
- ***Wartende?***

- ***Unsichere zivilrechtliche Lage...***

Internationales Recht im Auge behalten

- ***US Recht***
  - *Sammelklagen*
  - *Punitive Damages*

Automatisierte Systeme:
Rechtliche Kriterien der Einordnung: Haftung

Konsequenz Teil A:

- ***Konkrete Vereinbarungen über die Datennutzung sind nötig***
- ***Was soll das Produkt können? Weniger kann mehr sein…***
- ***Abgrenzung der Verantwortung muss dokumentiert werden***
- ***Aufklärung des Patienten über Haftungsrisiken ist essentiell!***

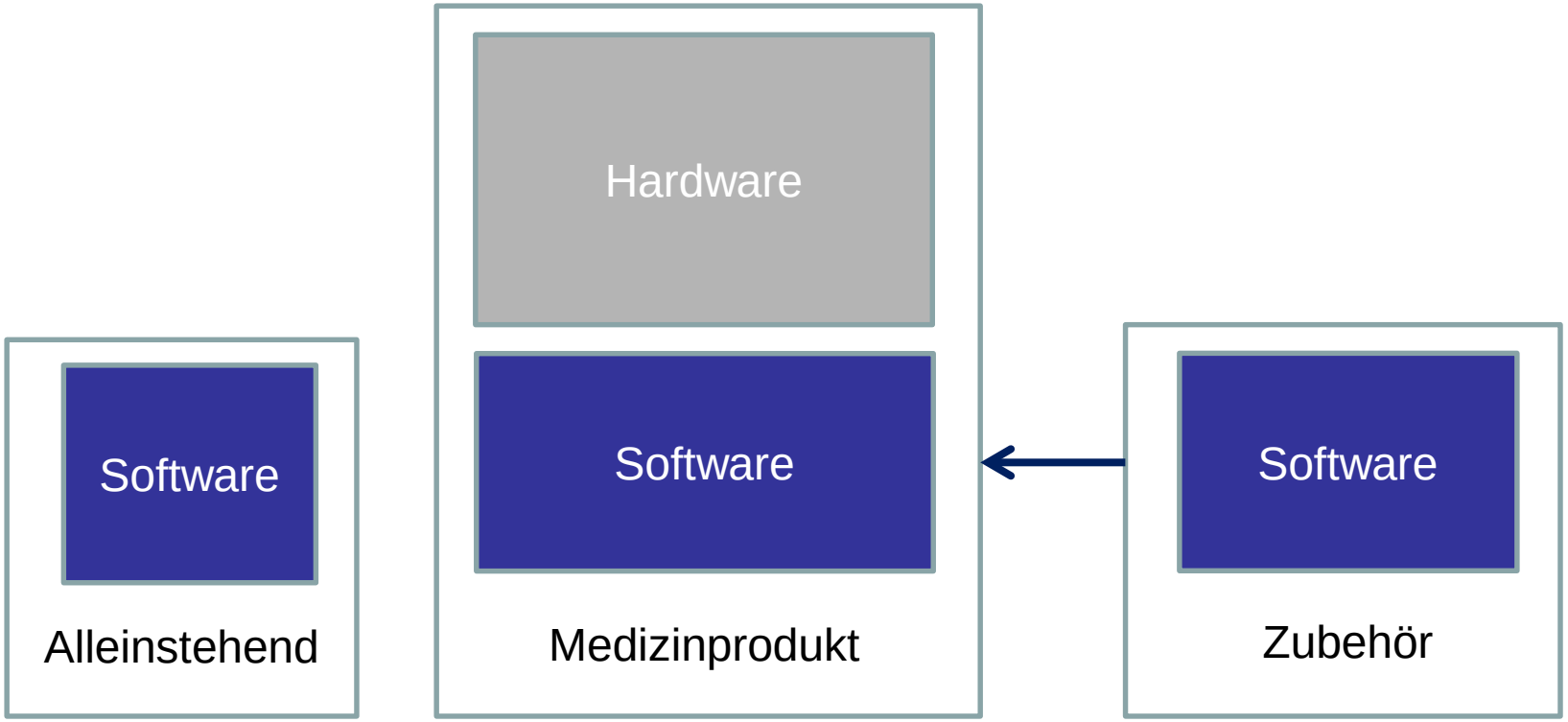
B. Einfluss des Softwarerechts

Welche Rahmenbedingungen gelten (außerhalb MDR) für Software und Apps im medizinischen Bereich?

- ***Software als Medizinprodukt ?***
- ***Neues Risiko: Rechtsmängel an Software***

B. Einfluss des Softwarerechts

Rahmenbedingungen Medizinprodukt



SW-Verträge und Rechteanalyse

Erwägungsgrund 19 MDR

Es muss eindeutig festgelegt werden, dass Software als solche, wenn sie vom Hersteller speziell für einen oder mehrere der in der Definition von Medizinprodukten genannten medizinischen Zwecke bestimmt ist, als Medizinprodukt gilt, während Software für allgemeine Zwecke, auch wenn sie in Einrichtungen des Gesundheitswesens eingesetzt wird, sowie Software, die für Zwecke in den Bereichen Lebensstil und Wohlbefinden eingesetzt wird, kein Medizinprodukt ist. Die Einstufung der Software entweder als Produkt oder als Zubehör ist unabhängig vom Ort der Software und von der Art der Verbindung zwischen der Software und einem Produkt.

Beispiele:

- Self-Tracking?
- Planung von Strahlentherapie ?
- KIS?
- PACS?

Software und Rechtsrahmen

Art 2 Nr. 1 MDR

„Medizinprodukt“ bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:
— Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,
— Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,
— Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,

Software und Rechtsrahmen

— Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.

Die folgenden Produkte gelten ebenfalls als Medizinprodukte:
— Produkte zur Empfängnisverhütung oder -förderung,
— Produkte, die speziell für die Reinigung, Desinfektion oder Sterilisation der in Artikel 1 Absatz 4 genannten Produkte und der in Absatz 1 dieses Spiegelstrichs genannten Produkte bestimmt sind.

-> Qualitätssicherungspflichten aus MDR greifen!

Software und Rechtsrahmen

25. „Kompatibilität“ bezeichnet die Fähigkeit eines Produkts — einschließlich Software —, bei Verwendung zusammen mit einem oder mehreren anderen Produkten gemäß seiner Zweckbestimmung
a) seine Leistung zu erbringen, ohne dass seine bestimmungsgemäße Leistungsfähigkeit verloren geht oder beeinträchtigt wird, und/oder
b) integriert zu werden und/oder seine Funktion zu erfüllen, ohne dass eine Veränderung oder Anpassung von Teilen der kombinierten Produkte erforderlich ist, und/oder
c) konfliktfrei und ohne Interferenzen oder nachteilige Wirkungen in dieser Kombination verwendet zu werden;

26. „Interoperabilität“ bezeichnet die Fähigkeit von zwei oder mehr Produkten — einschließlich Software — desselben Herstellers oder verschiedener Hersteller,
a) Informationen auszutauschen und die ausgetauschten Informationen für die korrekte Ausführung einer konkreten Funktion ohne Änderung des Inhalts der Daten zu nutzen und/oder
b) miteinander zu kommunizieren und/oder
c) bestimmungsgemäß zusammenzuarbeiten;

Software und Rechtsrahmen

14.2. Die Produkte werden so ausgelegt und hergestellt, dass folgende Risiken ausgeschlossen oder so weit wie möglich reduziert werden:
(...)
d)
Risiken im Zusammenhang mit der möglichen negativen Wechselwirkung zwischen Software und der IT-Umgebung, in der sie eingesetzt wird und mit der sie in Wechselwirkung steht;

Software und Rechtsrahmen

17. Programmierbare Elektroniksysteme — Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme gehören, und Produkte in Form einer Software

17.1. Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme, einschließlich Software, gehören, oder Produkte in Form einer Software werden so ausgelegt, dass Wiederholbarkeit, Zuverlässigkeit und Leistung entsprechend ihrer bestimmungsgemäßen Verwendung gewährleistet sind. Für den Fall des Erstauftretens eines Defekts sind geeignete Vorkehrungen zu treffen, um sich daraus ergebende Risiken oder Leistungsbeeinträchtigungen auszuschließen oder sie so weit wie möglich zu verringern.

17.2. Bei Produkten, zu deren Bestandteilen Software gehört, oder bei Produkten in Form einer Software wird die Software entsprechend dem Stand der Technik entwickelt und hergestellt, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschließlich der Informationssicherheit, der Verifizierung und der Validierung zu berücksichtigen sind.

Software und Rechtsrahmen

17. Programmierbare Elektroniksysteme — Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme gehören, und Produkte in Form einer Software

17.3. Bei der Auslegung und Herstellung der in diesem Abschnitt behandelten Software, die zur Verwendung in Verbindung mit mobilen Computerplattformen bestimmt ist, werden die spezifischen Eigenschaften der mobilen Plattform (z. B. Größe und Kontrastverhältnis des Bildschirms) und die externen Faktoren im Zusammenhang mit ihrer Verwendung (sich veränderndes Umfeld hinsichtlich Lichteinfall und Geräuschpegel) berücksichtigt.

17.4. Die Hersteller legen Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff fest, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind

Software und Rechtsrahmen

18. Aktive Produkte und mit diesen verbundene Produkte

18.1. Bei **nicht implantierbaren** aktiven Produkten sind für den Fall des Erstauftretens eines Defekts geeignete Vorkehrungen zu treffen, um sich daraus ergebende Risiken auszuschließen oder sie so weit wie möglich zu verringern.

18.2. Produkte mit interner Energiequelle, von der die Sicherheit des Patienten abhängt, werden mit einer Einrichtung, die eine Überprüfung des Ladezustands der Energiequelle gestattet, und einer geeigneten Warnvorrichtung oder Anzeige versehen, die aktiviert wird, wenn der Ladezustand der Energiequelle ein kritisches Niveau erreicht. Erforderlichenfalls wird die Warnvorrichtung oder Anzeige aktiviert, bevor der Ladezustand der Energiequelle ein kritisches Niveau erreicht.

18.3. Produkte mit externer Energiequelle, von der die Sicherheit des Patienten abhängt, werden mit einem Alarmsystem ausgestattet, das jeden Ausfall der Energiequelle signalisiert.

Software und Rechtsrahmen

18. Aktive Produkte und mit diesen verbundene Produkte

18.4. Produkte, die zur Überwachung eines oder mehrerer klinischer Parameter eines Patienten dienen, werden mit geeigneten Alarmsystemen ausgestattet, durch die der Anwender vor Situationen gewarnt wird, die den Tod oder eine erhebliche Verschlechterung des Gesundheitszustands des Patienten bewirken können.

18.5. Die Produkte werden so ausgelegt und hergestellt, dass die Gefahr der Entstehung elektromagnetischer Interferenzen, die das betreffende Produkt oder in der vorgesehenen Umgebung befindliche weitere Produkte oder Ausrüstungen in deren Funktion beeinträchtigen können, so weit wie möglich verringert wird.

18.6. Die Produkte werden so ausgelegt und hergestellt, dass sie eine Immunität gegenüber elektromagnetischen Interferenzen aufweisen, die einem bestimmungsgemäßen Betrieb angemessen ist.

18.7. Die Produkte werden so ausgelegt und hergestellt, dass das Risiko von unbeabsichtigten Stromstößen am Patienten, Anwender oder einem Dritten sowohl bei normaler Verwendung des Produkts als auch beim Erstauftreten eines Defekts so weit wie möglich ausgeschaltet wird, vorausgesetzt, das Produkt wird gemäß den Angaben des Herstellers installiert und instand gehalten.

18.8. Die Produkte werden so ausgelegt und hergestellt, dass sie so weit wie möglich vor einem unbefugten Zugriff, der das bestimmungsgemäße Funktionieren des Produkts behindern könnte, geschützt sind.

Software und Rechtsrahmen

19. Besondere Anforderungen für aktive implantierbare Produkte

19.1. Aktive implantierbare Produkte werden so ausgelegt und hergestellt, dass folgende Risiken ausgeschlossen oder so weit wie möglich verringert werden:
a) Risiken im Zusammenhang mit der Verwendung der Energiequellen, wobei bei der Verwendung von elektrischer Energie besonders auf Isolierung, Ableitströme und Erwärmung der Produkte zu achten ist,
b) Risiken im Zusammenhang mit medizinischen Eingriffen, insbesondere bei der Anwendung von Defibrillatoren oder Hochfrequenz-Chirurgiegeräten und
c) Risiken, die sich dadurch ergeben können, dass keine Wartung oder Kalibrierung vorgenommen werden kann(…)
19.2. Aktive implantierbare Produkte werden so ausgelegt und hergestellt, dass Folgendes gewährleistet ist:
— gegebenenfalls Verträglichkeit der Produkte mit den Stoffen, die sie abgeben sollen und
— Zuverlässigkeit der Energiequelle.

Software und Rechtsrahmen

19. Besondere Anforderungen für aktive implantierbare Produkte

19.3. Aktive implantierbare Produkte und gegebenenfalls ihre Bestandteile müssen identifizierbar sein, damit erforderlichenfalls nach Feststellung eines potenziellen Risikos im Zusammenhang mit den Produkten und ihren Bestandteilen die notwendigen Maßnahmen getroffen werden können.

19.4. Aktive implantierbare Produkte weisen einen Code auf, anhand dessen sie und ihr Hersteller eindeutig identifiziert werden können (insbesondere in Bezug auf Art des Produkts und Herstellungsjahr); es muss möglich sein, diesen Code erforderlichenfalls ohne chirurgischen Eingriff zu lesen.

Software und Rechtsrahmen

KAPITEL II
DURCHFÜHRUNGSVORSCHRIFTEN

3.3. Software, die ein Produkt steuert oder dessen Anwendung beeinflusst, wird derselben Klasse zugerechnet wie das Produkt.

Software und Rechtsrahmen

KAPITEL III
KLASSIFIZIERUNGSREGELN

6.3. Regel 11

Software, die dazu bestimmt ist, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, gehört zur Klasse IIa, es sei denn, diese Entscheidungen haben Auswirkungen, die Folgendes verursachen können:

— den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person; in diesem Fall wird sie der Klasse III zugeordnet, oder

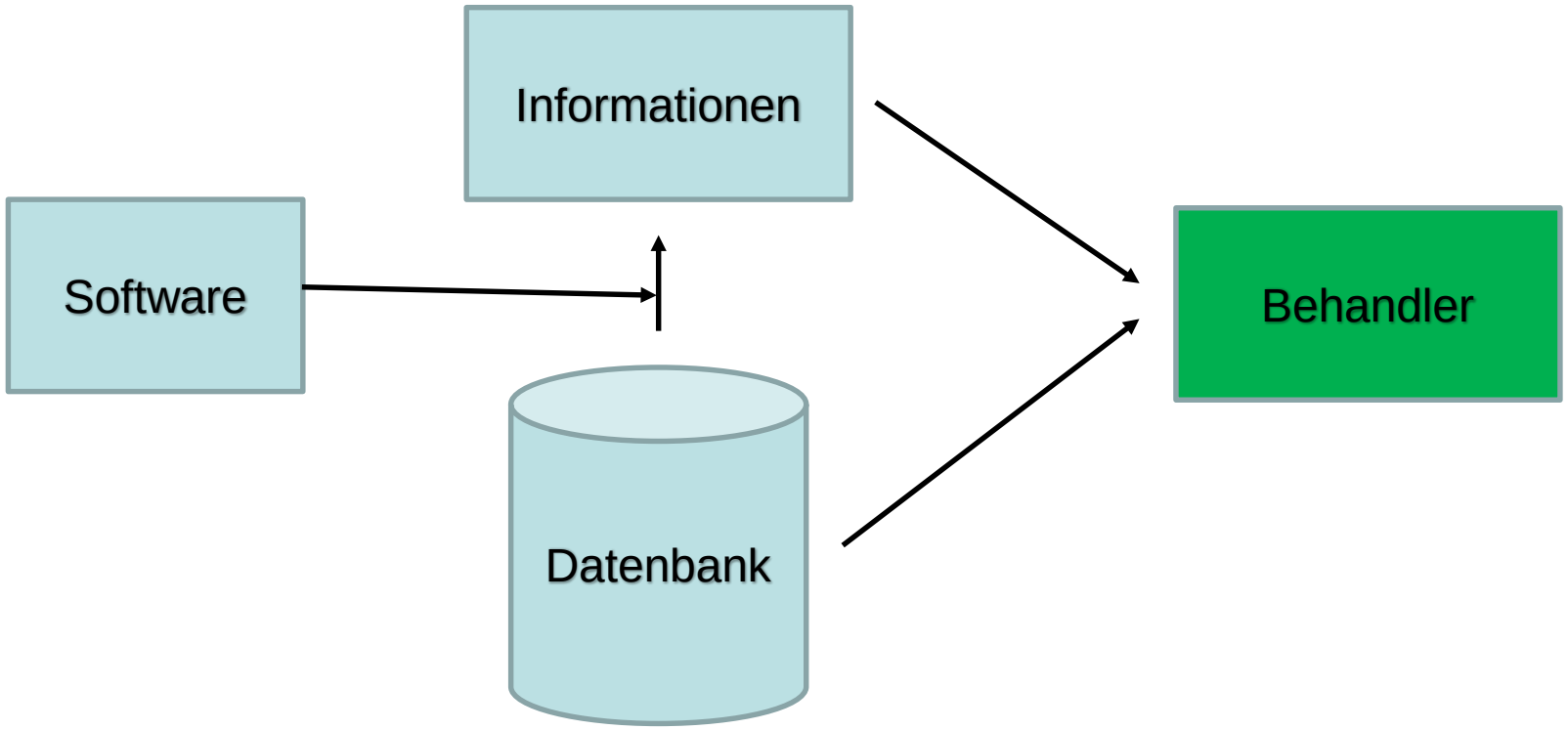
— eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person oder einen chirurgischen Eingriff; in diesem Fall wird sie der Klasse IIb zugeordnet.

Software, die für die Kontrolle von physiologischen Prozessen bestimmt ist, gehört zur Klasse IIa, es sei denn, sie ist für die Kontrolle von vitalen physiologischen Parametern bestimmt, wobei die Art der Änderung dieser Parameter zu einer unmittelbaren Gefahr für den Patienten führen könnte; in diesem Fall wird sie der Klasse IIb zugeordnet.

Sämtliche andere Software wird der Klasse I zugeordnet.

Software und Rechtsrahmen

KAPITEL III KLASSIFIZIERUNGSREGELN
Welche Software gehört dann noch zur Klasse I?
„Sämtliche andere Software wird der Klasse I zugeordnet.“



Versuch: Nicht Informationen liefern, sondern interpretierbare Daten:..
https://www.linkedin.com/pulse/mdr-rule10a-really-wrong-tobias-schreiegg/

SW-Verträge und Rechteanalyse

Empfehlung: https://www.johner-institut.de/blog/regulatory-affairs/mdr-regel-11/

Produkt	Klasse MDR
App zur Auswahl und zur Dosisberechnung von Cytostatika	III
Stand-alone Software-Anwendung für die AMTS	III (je nach Medikament)
Software zum Vorschlagen von Diagnosen basierend auf Laborwerten	IIb oder höher (bis III)
PDMS	IIb oder III
App zur Diagnose von Schlafapnoe	IIa (oder höher)
Software für die Therapie- bzw. Bestrahlungsplanung	IIb oder III, je nach Argumentation

Software und Rechtsrahmen

KAPITEL III
KLASSIFIZIERUNGSREGELN

Wann ist Software, NICHT dazu bestimmt, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, gehört zur Klasse IIa, es sei denn, diese Entscheidungen haben Auswirkungen, die Folgendes verursachen können:
— den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person; in diesem Fall wird sie der Klasse III zugeordnet, oder
— eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person oder einen chirurgischen Eingriff; in diesem Fall wird sie der Klasse IIb zugeordnet.

Diskussionsmodell?

- Monitoring
- Prävention
- Linderung
- Prognosen (nicht entscheidungsrelevant)

Software und Rechtsrahmen

KAPITEL III
KLASSIFIZIERUNGSREGELN

Entscheidend ist die Bestimmung!

- Was ist offizieller Zweck der App / der Software?

- Bleibt der Arzt oder Patient Entscheider? Oder wird Verantwortung abgenommen?

- Wird in Therapie oder Behandlung eingegriffen?

- Klasse I, wenn Software mit den verarbeiteten Informationen unmittelbar zur Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen wird.

SW-Verträge und Rechteanalyse

Rechtliche Risiken, die zu vermeiden sind:

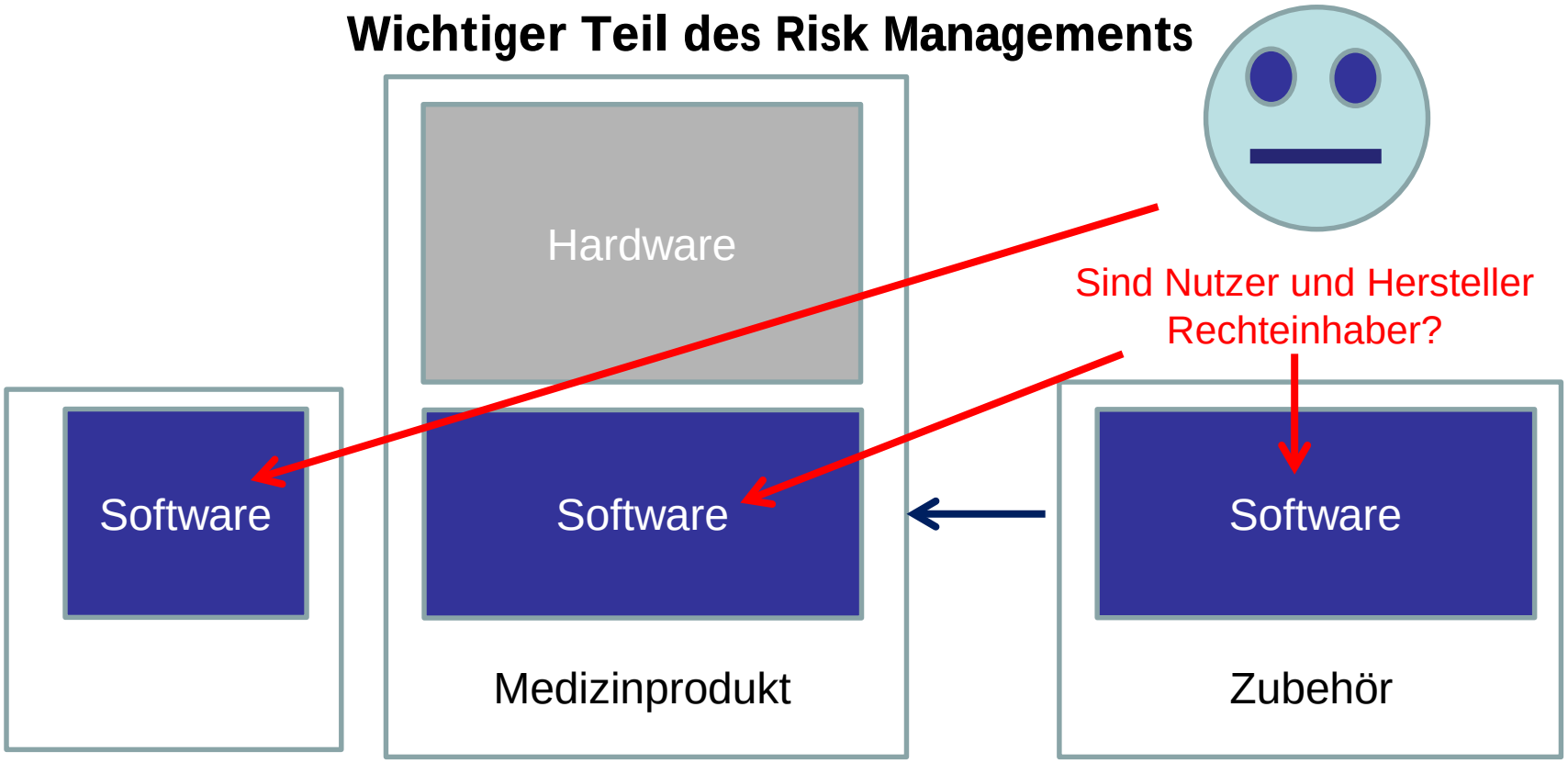
- **Verstöße gegen die MDR, aber auch**
  - **Unterlassungsansprüche wegen fehlender Produktrechte**
  - **Unterlassungsansprüche aus dem Datenschutz**

  - **Im Folgenden:**

    Problem der Betriebssicherheit bei Lizenzverstößen

Software und Rechteanalyse

IT&IP Due Diligence Medizinprodukt:
Wichtiger Teil des Risk Managements



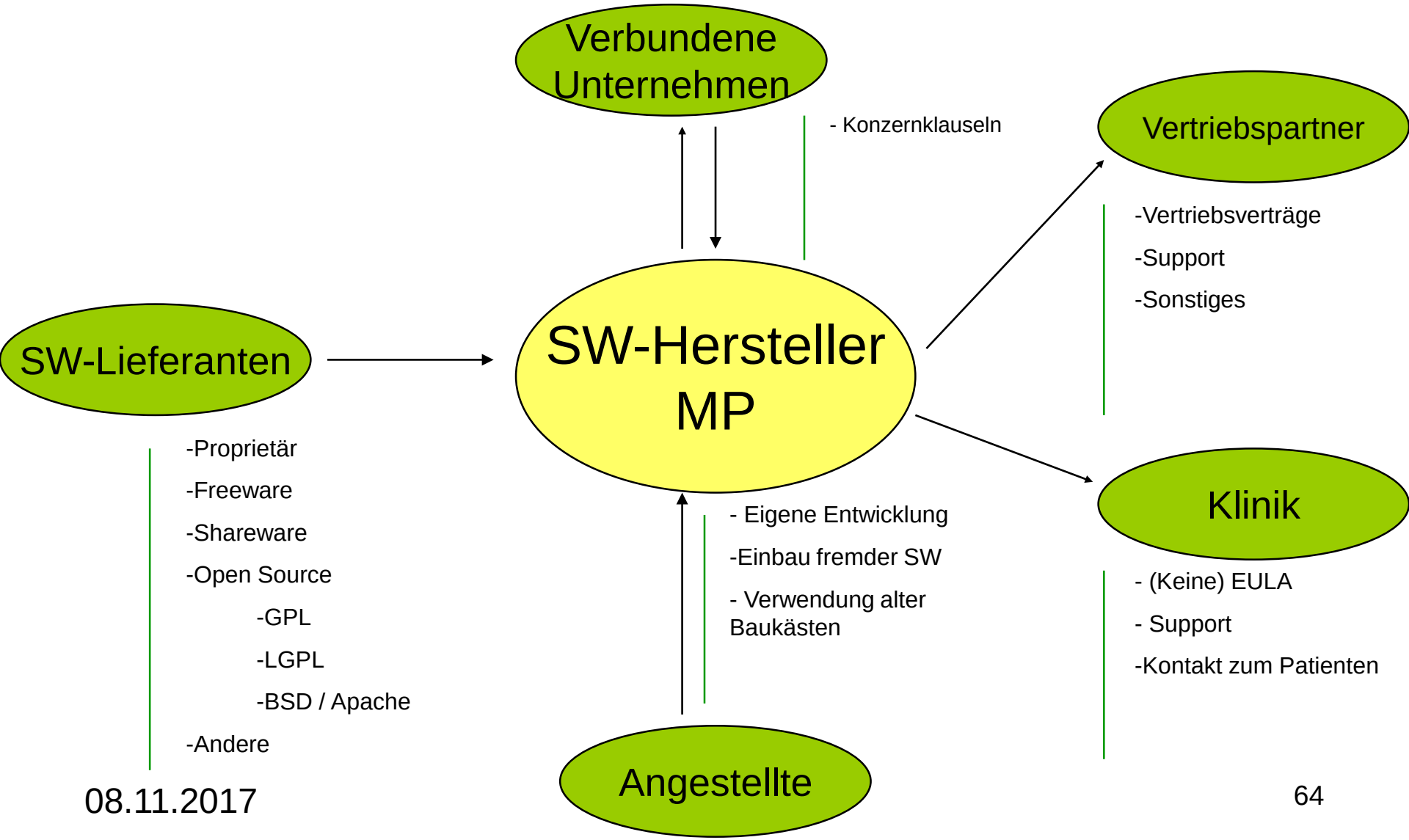
SW-Verträge und Rechteanalyse

- **Mögliche Rechte an Software**
  - Patente ?
  - Urheberrechte ?
    - Proprietäre Lizenzen
    - Freeware
    - Shareware
    - Open source
    - Sonstige
  - Markenrechte?
  - Wettbewerbsrecht?
  - Andere vertragliche Verpflichtungen…

Herausforderungen

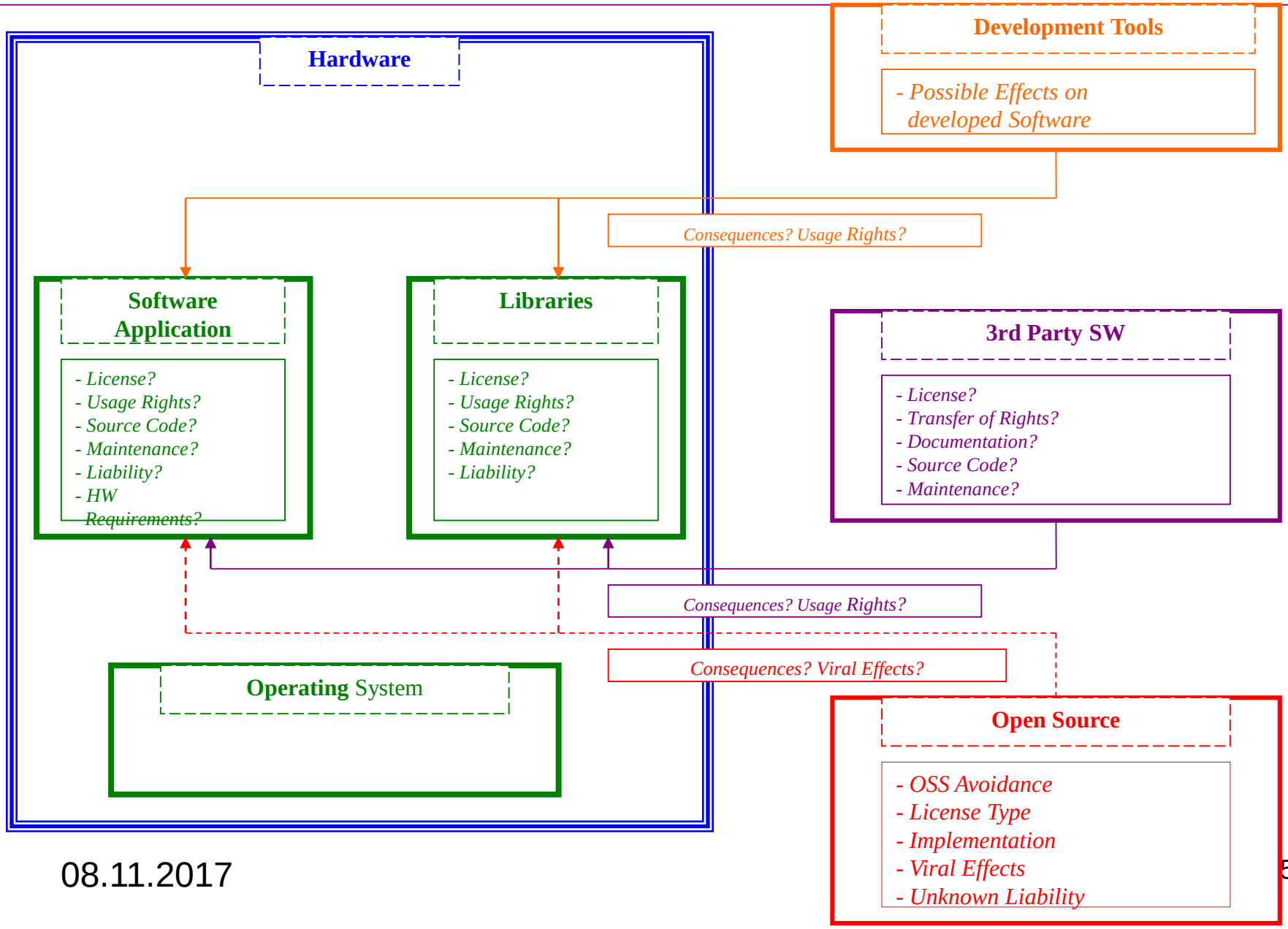
- **Mögliche Rechteinhaber**
  - Software-Lieferanten
    - traditionell oder
    - free lancer
  - Angestellte
  - Andere
    - Freeware- / Shareware- / Open-Source -Entwickler

Rechtediagramm: Beteiligte



Rechtediagramm: Technisch

Institut für Informationsrecht



Rechteanalyse: Fragen

Institut für Informationsrecht

Vergleich vorhandener und benötigter Rechte

- **Welche Rechte benötige ich?**
  - aufgrund
    - Eigener Nutzung
    - Vergebener Rechte an
      - » Verbundene Unternehmen
      - » Vertriebspartner
      - » Klinik
- **Welche Rechte sind vorhanden?**
  - Aufgrund von Vereinbarungen mit
    - Softwarelieferanten
    - Angestellten Programmierern

Vorgehensmodell

- **Schritt 1: Definition benötigter Rechte**
- **Schritt 2: Analyse vorhandener Rechte**
- **Schritt 3: Lückenschluß**

SW-Verträge und Rechteanalyse

- **Schritt 1: Definition benötigter Rechte**
  - Klärung der für die medizinische Nutzung (ggf. im Verbund) benötigten Rechte
  - Klärung des Lizenzmodells, d.h.
    - Exklusivität
    - Territorium
    - Befristung
    - Gebühren
    - Support
    - Nutzungsrechtsbeschränkungen
    - Bearbeitungsrechte
    - Gewährleistungsrechte, Haftung

SW-Verträge und Rechteanalyse

- **Schritt 2: Analyse vorhandener Rechte**
  - Rechteerwerb von
    - Verbundenen Unternehmen
    - SW-Lieferanten
    - Angestellten
  - Klärung der Rechtsfolgen von Open-Source-Software-Einbau wie
    - Unbekannte Entwickler
    - Folgen von Lizenzverletzungen
    - virale Effekte
    - Gewährleistung und Haftung

SW-Verträge und Rechteanalyse

- **Step 2: Analyse vorhandener Rechte**
  - **Folgen von Lizenzverletzungen**
    - Unterlassungsansprüche
    - Teurer Rechtenachkauf
  - **virale Effekte**
    - GPL 2.0: Offenlegung eigenen Quellcodes
  - **Gewährleistung und Haftung**

SW-Verträge und Rechteanalyse

- **Freeware**
  - **Alles was nichts kostet**
- **Shareware**
  - Alles, was nicht richtig oder nicht lange funktioniert
- **Open Source**
  - **Alles was nichts kostet, mit offenem Quellcode**

SW-Verträge und Rechteanalyse

- **Bedeutung des Quellcodes**

view-source:http://www.fernhilfe.ch/

Meistbesucht Web Slice-Katalog Erste Schritte Outlook Web App

```
<html>

    <head>
        <meta http-equiv="content-type" content="text/html;charset=iso-8859-1">
        <title>Geistheiler seit 1980 &#150; Geistheilung bei k&ouml;rperlichen und seelischen Pro
        <meta name="keywords" content="Lebenshilfe, Lebensberatung, Hilfe, Helfer, Geisthelfen, G
        <meta name="verify-v1" content="Q6SowfkcF9CmCrpj+kkYUTBxaeZbesBlWwOiF2Bw5oA=" />
        <meta name="verify-v1" content="sl9raYI3VSZ/0PLsKIXcJBiQC0VGPFXxgz0cwIAHP2s="/>
        <meta name="verify-v1" content="1CvpOkksEZnBK4P5FDwY6oWWmJ/XEjM+mX70DIFagGc="/>

    <!-- Google Analyticscode Code for www.fernhilfe.ch for Tracking-ID: UA-38320770 START -->
<script type="text/javascript">
  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-38320770-1']);
  _gaq.push(['_setDomainName', 'fernhilfe.ch']);
  _gaq.push(['_setAllowLinker', true]);
  _gaq.push(['_trackPageview']);
 (function() {
    var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
    ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-a
    var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
  })();
</script>
<!-- Google Analyticscode Code for www.fernhilfe.ch for Tracking-ID: UA-38320770 END -->
```

SW-Verträge und Rechteanalyse

Freeware

- **Kostenlose Lizenzen**
- **Quellcode liegt nicht offen**
- **Proprietäre Software**
- **Häufige Vorgaben der Lizenz**
  - Namensnennung
    - Innerhalb des Programms
    - In Werbematerialien
    - Auf der Homepage des Verwenders
  - Kennzeichnung von Veränderungen
  - Gewährleistungs- und Haftungsausschluß
  - Teilweise Ausschluß kommerzieller Nutzung
  - Keine Veränderung von Lizenzhinweisen des Urhebers

SW-Verträge und Rechteanalyse

Freeware: Beispiel

- Copyright (C) 1997-2006 by François PIETTE Rue de Grady 24, 4053 Embourg, Belgium francois.piette@overbyte.be Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented, you must not claim that you wrote the original software. (...) 4. **You must register this software by sending a picture postcard to the author. Use a nice stamp and mention your name, street address, EMail address and any comment you like to say.**

SW-Verträge und Rechteanalyse

Freeware: Beispiel

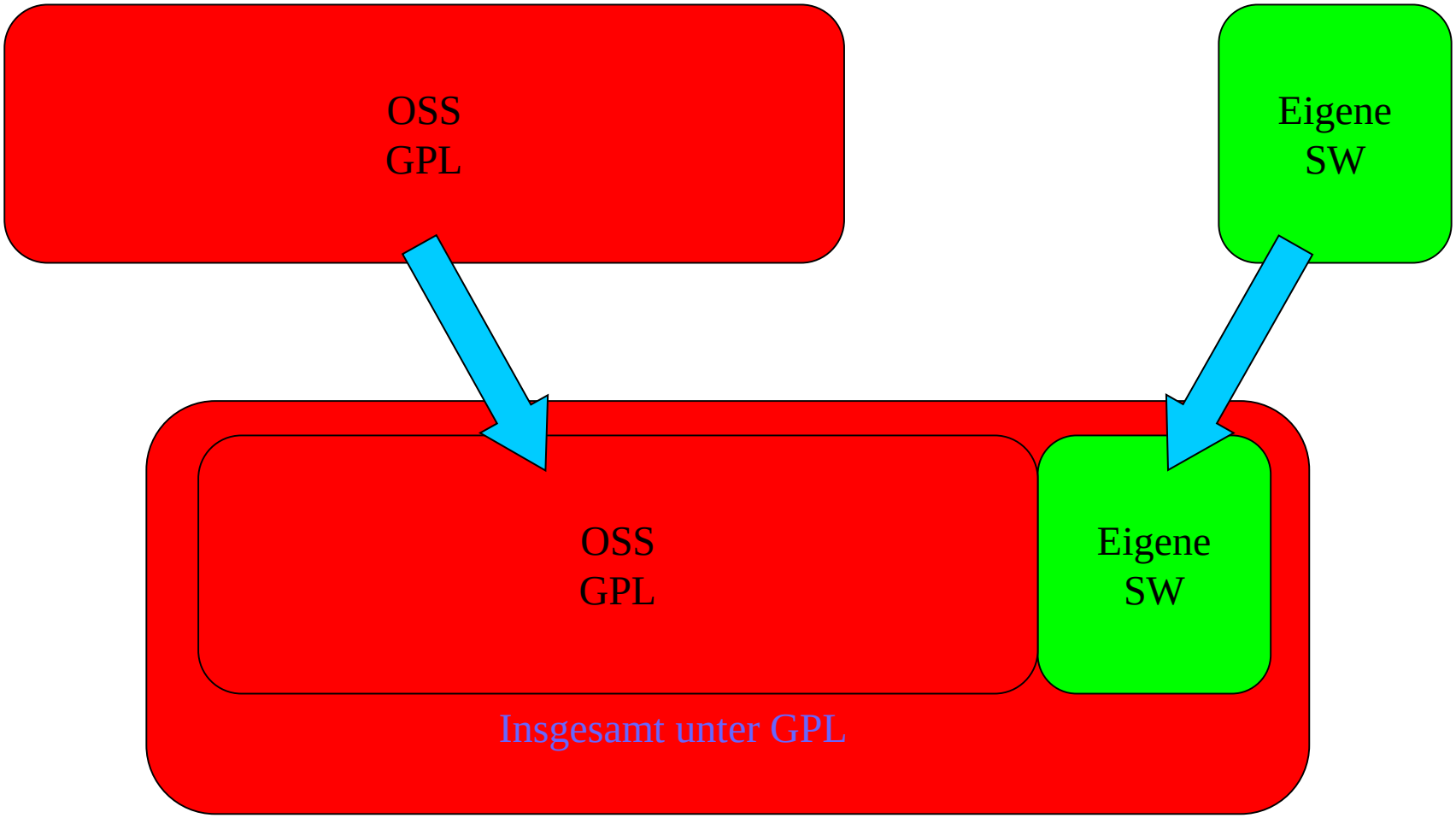
DO WHAT THE HELL YOU WANT TO PUBLIC LICENSE Version 2, December 2004

- Copyright (C) 2004 Sam Hocevar 14 rue de Plaisance, 75014 Paris, France
- Everyone is permitted to copy and distribute verbatim or modified copies of this license document, and changing it is allowed as long as the name is changed.

- 0. DO WHAT THE HELL YOU WANT TO PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

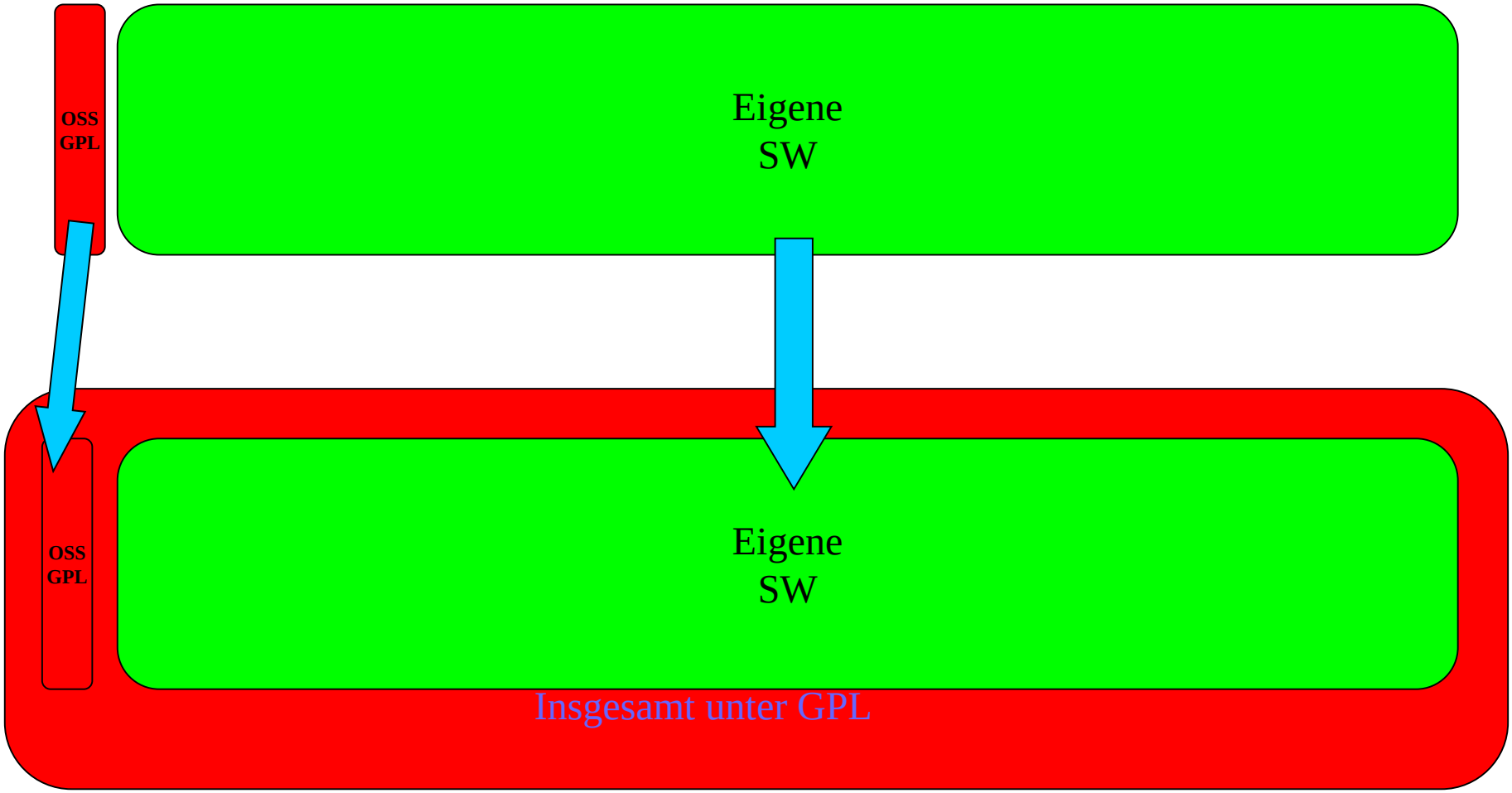
- 0. You just DO WHAT THE HELL YOU WANT TO

SCHEMA
Software-Nutzung unter strengem Copyleft / GPL 2.0

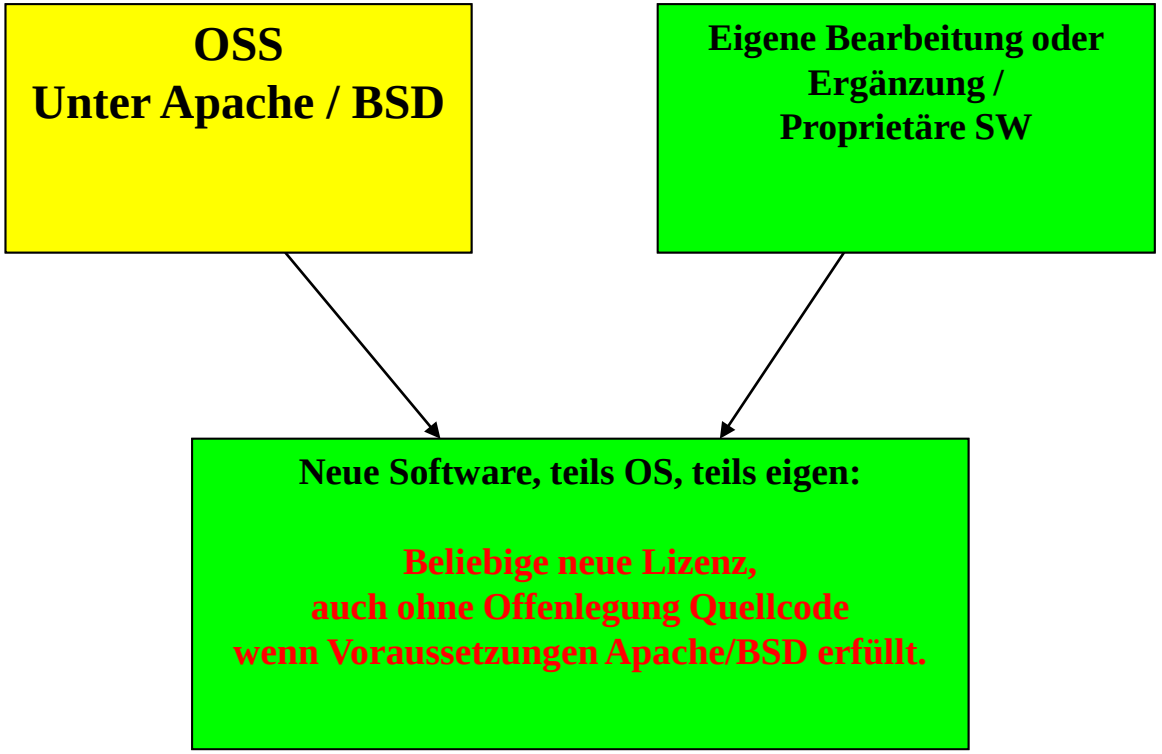


08.11.2017
76

SCHEMA
Software-Nutzung unter strengem Copyleft / GPL 2.0



SCHEMA
Software-Nutzung von OSS ohne Copyleft (Apache / BSD)



08.11.2017
78

SW-Verträge und Rechteanalyse

- **Was ist zu vermeiden?**
  - **Ein Risiko einer „Infektion“ proprietärer Software durch Einbindung von Open-Source-Software (OSS) besteht dann, wenn die OSS unter der falschen Lizenz steht.**
  - **Nur unter einer der gängigsten 3 Lizenztypen kann OSS mit proprietärer Software verbunden oder bearbeitet und dann unter beliebiger anderer Lizenz weiterverbreitet werden (wenn bestimmte Urheberrechtshinweise erhalten bleiben).**
  - **Bei der verbreitetsten und strengsten Lizenz (GPL) führt die Einbindung von OSS dazu, dass das Softwareprodukt nur unter dieser Lizenz (unter Offenlegung des Quellcodes) weitervertrieben werden kann.**
  - GEFAHR DER UNTERSAGUNG DES EINSATZES DES MEDIZINPRODUKTS

Lösungen: Lücke schließen

- **Schritt 3:**
  Lücke schließen

  - **Gleiche SW mit besseren Rechten erwerben?**
    - Lieferantenverträge ändern
  - **Weniger Rechte herausgeben?**
    - Änderung von Vertriebsverträgen und EULA
  - **Andere SW mit besseren Rechten erwerben?**

Lösungen: Lücke schließen

- **Schritt 3:**
  Lücke schließen
  - **Andere SW mit besseren Rechten erwerben?**
  - **Darf ich das vertraglich?**

Lösungen: Lücke schließen

- **Schritt 3:**
  Lücke schließen

  - **Als Hersteller: Aufsetzen eines Prozesses, um**
    - **die Lücke zu schließen (Schritte 1 bis 3)**
    - **fortlaufende ein- und ausgehende Rechte zu beobachten**
    - **herausgehende Rechte an eingehende Rechte ggf. anzupassen**
    - **möglichen Einbau von Open Source zu prüfen**
    - **internationale Rechtsunterschiede im Auge zu behalten**

    - **Als Endkunde:**

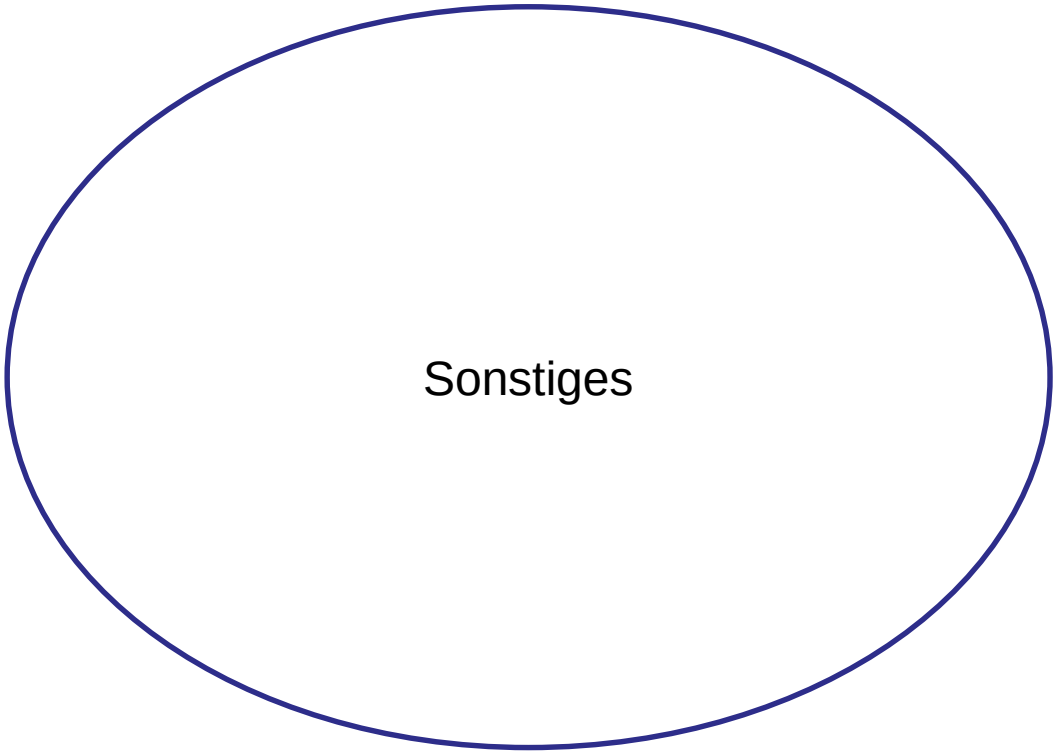
  - **Nachweis der obigen Maßnahmen vereinbaren**

C. Datenschutz

- **Datenschutzgrundlagen**
- **Datenschutz und smarte Medizin**
- **DSGVO und DSG 2018**

Datenschutz

- **Datenschutz früher**



1. Einführung in den Datenschutz
Was sind geschützte Daten?

Begrifflichkeiten und Entstehungsgeschichte

„Jeder muss wissen, wer was wann wo und bei welcher Gelegenheit über ihn weiß.“

2 Grundrechte:

- Recht auf informationelle Selbstbestimmung
- Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

1. Einführung in den Datenschutz: Was sind geschützte Daten?

Begrifflichkeiten und Entstehungsgeschichte

Ich muss daher unter anderem wissen (können):

- Wem habe ich meine Daten gegeben?
- Zu welchem Zweck?
- An wen wurden die Daten weitergegeben?
- Wurden sie verändert?
- Wann werden sie gelöscht?

1. Einführung in den Datenschutz: Was sind geschützte Daten?

Begrifflichkeiten:

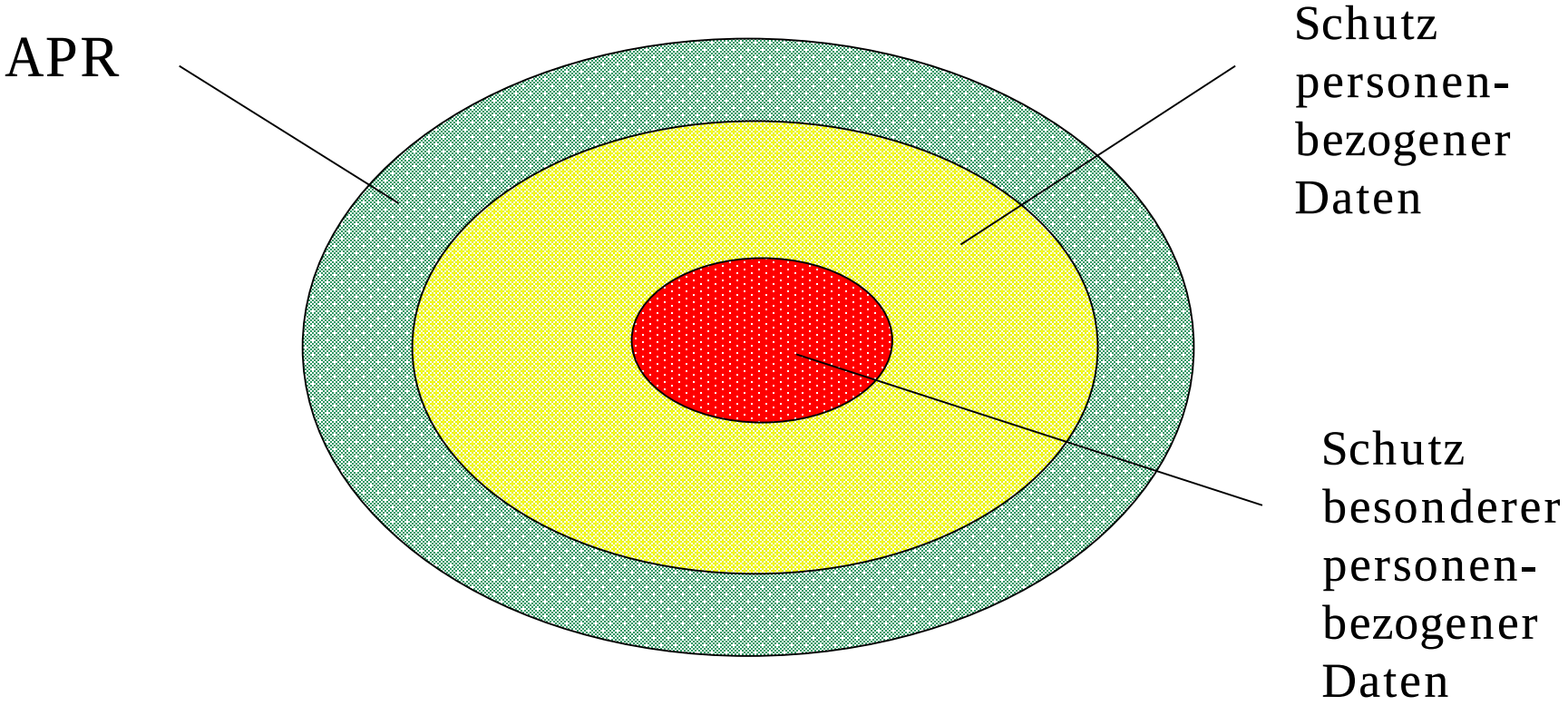
- Allgemeines Persönlichkeitsrecht
- Personenbezogene Daten,
- besondere Personenbezogene Daten

Im weiteren Sinne:

- Geheimnisschutz,
- Vertrauliche Daten aufgrund NDA
- Eigenes Know-How

1. Einführung in den Datenschutz: Was sind geschützte Daten?

Begrifflichkeiten: Allgemeines Persönlichkeitsrecht (APR)



Institut für Informationsrecht

1. Einführung in den Datenschutz: Was sind geschützte Daten?

Begrifflichkeiten: Entstehungsgeschichte

Ich muss unter anderem wissen (können):

Wer hat woher meine Daten?

- Beispiel: Eine Fluggesellschaft veräußert die Daten
  - der männlichen Vielflieger, die
  - auch auf Kurzstrecken
  - immer Gangplätze gebucht haben
  - und über 50 Jahre alt sind

- aber an wen?...

Institut für Informationsrecht

1. Einführung in den Datenschutz: Was sind geschützte Daten?

- Begrifflichkeiten: Was sind **personenbezogene Daten:**

- **„Einzelangaben über**

➢ **persönliche oder sachliche Verhältnisse**
➢ **einer bestimmten oder**
➢ **bestimmbaren (mit vertretbarem Aufwand ermittelbaren)**
➢ **natürlichen Person“**

➢ **„GesamtIQ des 4-köpfigen Teams bei 350“ (Verfügbares Zusatzwissen !)**
➢ **Fallnummer?**
➢ **Daten eines Implantats?**
➢ **Behandelnde Ärztin?**
➢ **Daten oder auch Kommentare meiner Kollegen?**
➢ **Der Name einer Person selbst?**
➢ **Die Adresse einer Person?**

Institut für Informationsrecht

1. Einführung in den Datenschutz

- Begrifflichkeiten: **Besondere Personenbezogene Daten**:

- personenbezogene 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.

- Welche religiösen Daten werden im Krankenhaus erfaßt?

- Mögliche Zwecke?

Institut für Informationsrecht

1. Einführung in den Datenschutz

- Begrifflichkeiten: **Besondere Personenbezogene Daten**:

- Mögliche Zwecke?

- Behandlung / Krankenhausvertrag?
- Aus- und Fortbildung?
- Qualitätssicherung?
- Forschung?
- Abrechnung?
- Weitergabe an andere Behandler?
- Verkauf von Daten?

1. Einführung in den Datenschutz

Institut für Informationsrecht

- Umgang mit Daten: Was kann man mit den Daten tun?

  - Es gelten besondere Regelungen für

    - besondere personenbezogene Daten
    - Geheimnisschutz
    - Übermittlung in Drittstaaten
    - Automatisierte Einzelentscheidungen
    - Videoüberwachung
    - Mobile Speicher- und Verarbeitungsmedien
    - Personaldaten (Einstellung, Personalakte)

1. Einführung in den Datenschutz

Umgang mit Daten: Wann zulässig?

Grundregel:

§ 4 BDSG Zulässigkeit der Datenverarbeitung und -nutzung

Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

§ 4a BDSG

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

1. Einführung in den Datenschutz

- Umgang mit Daten: Woher beziehe ich die Berechtigung?

- **Verbot mit Erlaubnisvorbehalt:**
- **Drei Möglichkeiten der Berechtigung:**

1. Einwilligung oder
2. Gesetz (verfassungskonform!) oder
   - zB.: BDSG, TMG, Krankenhausfinanzierungsgesetz, StPO, TKG...
3. Facebook-Klausel
   - Daten waren allgemein zugänglich...

1. Einführung in den Datenschutz

•Umgang mit Daten: Woher beziehe ich die Berechtigung?

•Einwilligungsvoraussetzungen

- Die Einwilligung setzt rechtmäßige Information und Freiwilligkeit voraus
- Die Einwilligung umfasst
  - automatisch das, was im Rahmen der Zweckbestimmung der Vertragserfüllung zwingend notwendig ist, aber darüber hinaus nur
  - die explizit angekündigten Zwecke!

1. Einführung in den Datenschutz

•Umgang mit Daten: Woher beziehe ich die Berechtigung?

•Einwilligungsvoraussetzungen

➢ **§ 4 BDSG Zulässigkeit der Datenverarbeitung und -nutzung**

•(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

1. Einführung in den Datenschutz

Umgang mit Daten

Einwilligungsgrundsätze: Vertragszweck oder nicht?

§ 28 Datenspeicherung, übermittlung und -nutzung für eigene Zwecke

(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,

2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt,

1. Einführung in den Datenschutz

- **Umgang mit Daten**
- **Einwilligungsgrundsätze: Allgemein zugängliche Quellen**

- **§ 28 Datenspeicherung, übermittlung und -nutzung für eigene Zwecke**
- **(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig**
- **3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung offensichtlich überwiegt,**
- **4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist.**
- **Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.**

1. Einführung in den Datenschutz

- Umgang mit Daten:
- Woher beziehe ich die Berechtigung?

Beispiel Einwilligung

- **Logik des Einwilligungsumfangs**

➢ Welche Daten und Zwecke sind automatisch von der Bestellung im Onlineshop mit Lastschrift umfaßt?

➢ Welche Daten sind automatisch von der Newsletterbestellung erfaßt?

1. Einführung in den Datenschutz

•Umgang mit Daten:
•Woher beziehe ich die Berechtigung?

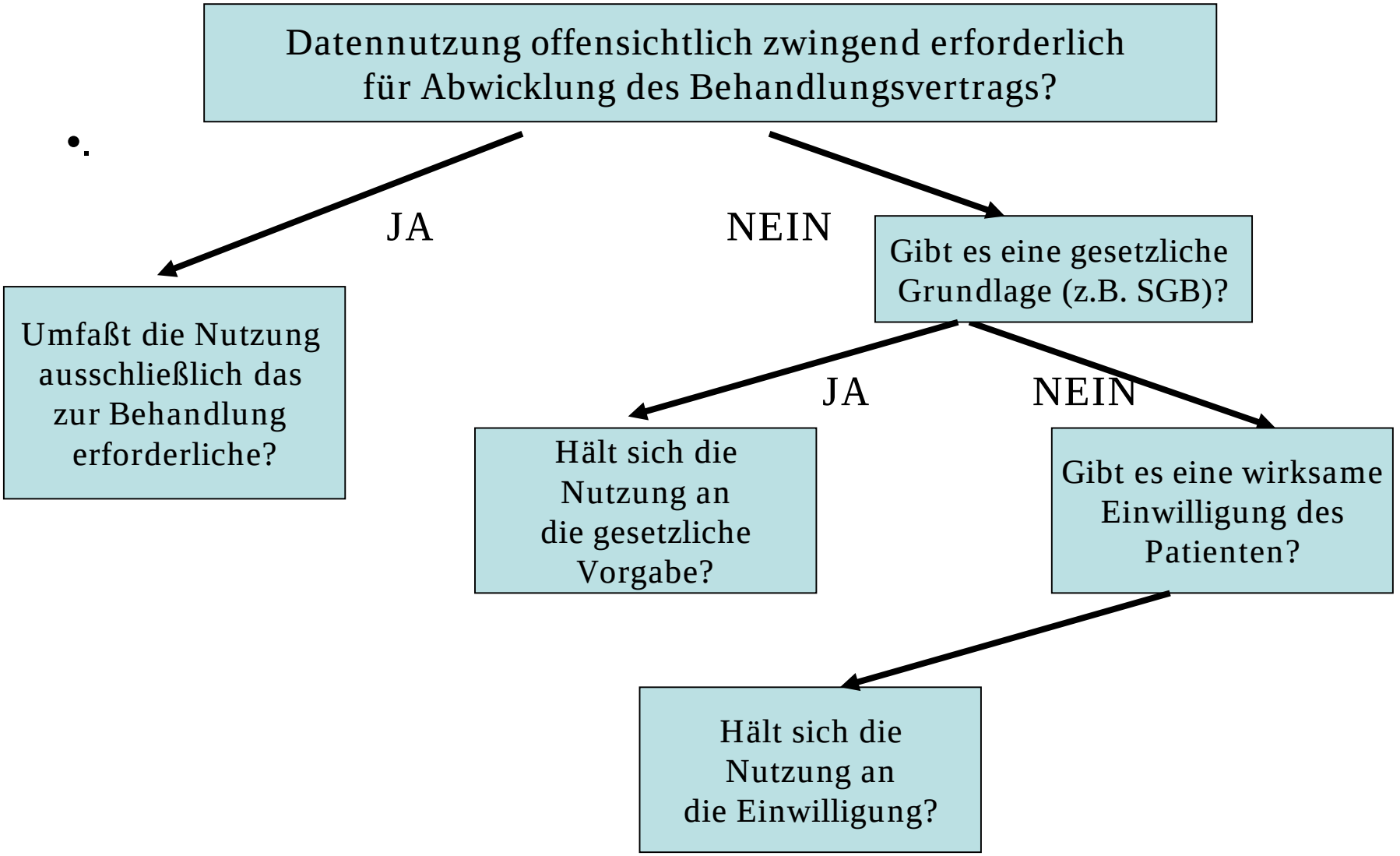
Beispiel GESETZ

•Berechtigungen aus § 73 Abs. 1b Sozialgesetzbuch V (SGB V)

•(1b) Ein Hausarzt darf mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die einen Versicherten behandelnden Leistungserbringer sind verpflichtet, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die in Satz 1 genannten Daten zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln; die behandelnden Leistungserbringer sind berechtigt, mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu erheben und für die Zwecke der von ihnen zu erbringenden Leistungen zu verarbeiten und zu nutzen.

1. Einführung in den Datenschutz

Wann darf ich Patientendaten verarbeiten?



1. Einführung in den Datenschutz

- Konsequenz:

- Daten, die bei der Aufnahme erhoben werden und NICHT zwingend für die Behandlung erforderlich sind, können nur auf Basis einer freiwilligen Einwilligung erhoben werden.

1. Einführung in den Datenschutz

- Umgang mit Daten:

Umgang mit besonderen personenbezogenen Daten (Berufsgeheimnis):

§ 39 BDSG Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

1. Einführung in den Datenschutz

Eingangsbereich Klinikum und Abteilungen:
Sonderproblem Videoüberwachung

Wenn dies zur

1. Wahrnehmung des Hausrechts oder
2. Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass **schutzwürdige Interessen der Betroffenen** überwiegen.

Problem der Kombination mit automatisierten Verfahren:

– Vergrößern und Herausfiltern einzelner Personen,
– biometrischen Erkennung,
– Profilerstellung.

1. Einführung in den Datenschutz

- Klassische Datenschutzthemen im Medizinbereich

- Erforderlichkeit der Datenerhebung: Das „Dr. House-Dilemma“: Welche Daten werden zukünftig erforderlich werden?
- Datentransfer in medizinischen Netzen:
  - WebEPA
  - Fallakte
  - Datenweitergabe an (potenzielle) Weiterbehandler
- Zusatzanforderungen der ärztlichen Schweigepflicht
- Regelvorliegen „besonderer personenbezogener Daten“

1. Einführung in den Datenschutz

- Notwendigkeit von Vorabkontrollen / künftig Datenschutzfolgeabschätzung

Vorabkontrollen sind durchzuführen nach§ 4d Abs. 5 Satz 2 BDSG, wenn

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden (Nr. 1) oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten, einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens (Nr. 2).

(Beispiel: Scoring-Systeme, Testverfahren, Provisionsbewertungen)

1. Einführung in den Datenschutz

- Rechtzeitige Einschaltung des Datenschutzbeauftragten
- zur Ermöglichung von Vorabkontrollen
- zur Erstellung der Verfahrensverzeichnisses
- in Zweifelsfragen zur Abklärung und Vermeidung von Beschwerden durch Betroffene

1. Einführung in den Datenschutz

•Begrifflichkeiten: vertrauliche Daten aufgrund NDA

-Typisches NDA (gegenseitig oder einseitig).

- Definition der vertraulichen Informationen
- Definition der Verletzungshandlungen
- Löschungspflichten
- **Vertragsstrafe bei Verletzung!**

1. Einführung in den Datenschutz Geheimnisschutz

- Geregelt u.a.
- **§ 203 StGB** - Verletzung von Privatgeheimnissen
  Bis zu zwei Jahren Freiheitsstrafe
- **§ 17 UWG** – Verrat von Geschäfts- und Betriebsgeheimnissen
- **§ 5 BDSG -** (Datengeheimnis)
- **§ 44 BDSG** – Bis zu zwei Jahren Freiheitsstrafe
- **§ 9 BOÄ** Niedersachsen „Patientengeheimnis“.

1. Einführung in den Datenschutz Geheimnisschutz

Institut für Informationsrecht

- **ULD „Patientendatenschutz im Krankenhaus“**
- **https://www.datenschutzzentrum.de/medizin/krankenh/patdskh.htm**

- „Das Patientengeheimnis umfasst alle Informationen, die mit der ärztlichen Behandlung in Zusammenhang stehen. Dazu gehört die Art der Krankheit, deren Verlauf, Anamnese, Diagnose, Therapie und Prognose, körperliche und geistige Feststellungen, gehören Patientendaten in Akten und auf elektronischen Datenträgern, Untersuchungsmaterial und Untersuchungsergebnisse. Dazu gehören aber auch sämtliche im Rahmen der Behandlung bekannt gemachten Angaben über persönliche, familiäre, berufliche, wirtschaftliche und finanzielle Gegebenheiten, auch wenn diese keinen direkten Bezug zu einer Krankheit haben. Schon der Name oder die Tatsache der Behandlung des Patienten stellt ein Patientengeheimnis dar. Geschützt werden auch Informationen über Dritte, die der Patient dem Arzt anvertraut.“

1. Einführung in den Datenschutz Geheimnisschutz

§ 203 Verletzung von Privatgeheimnissen

(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,

…

(3) (...) Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen (...) gleich.

(z.B. Pflegedienst, Klinikapotheke, Krankenhausverwaltung, Krankenhausarchivs, EDV-Abteilung)

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft

1. Einführung in den Datenschutz Geheimnisschutz

Fremde Geheimnisse i.S.d. **§203 StGB** sind nur Privatgeheimnisse, d.h. solche Tatsachen, die nur einem beschränkten Personenkreis bekannt sind und nach dem verständlichen Interesse des Geheimnisträgers nicht weiter bekannt werden sollen

•Eine Tatsache verliert den Geheimnischarakter nicht notwendig, wenn sie schon einmal verraten worden oder gerüchtweise bekannt geworden ist

1. Einführung in den Datenschutz Geheimnisschutz

Offenbaren i.S.d. **§203 StGB:**

Jemandem direkt oder konkludent eine Geheimnis oder eine Einzelangabe mitteilen, die diesem

-**nicht,**

-**nicht in diesem Umfang,**

-**nicht sicher** oder

-**nicht in dieser Form**

bekannt war...

1. Einführung in den Datenschutz Geheimnisschutz

Offenbaren i.S.d. **§203 StGB:**

Es genügt die Angabe
-der Tatsache und von
-Einzelangaben, die die Identifikation der Person ermöglichen.

-Die Einräumung einer Zugriffsmöglichkeit genügt;
-auch ein Unterlassen der Sicherung ist ausreichende Tathandlung...

1. Einführung in den Datenschutz Geheimnisschutz

- **Weitergabe an Nicht-Mitbehandler?**

Eine Strafbarkeit i.S.d. §203 StGB kann auch bei Offenbarung gegenüber anderen Behandlern vorliegen, welche ebenfalls der Schweigepflicht unterliegen, BGHZ 116, 268; LG München I, Urteil vom 1.10.1993; Az.: 23 O 2157/91.

Aber : Kein Offenbaren bei Weitergabe innerhalb des “Kreises der Wissenden”

1. Einführung in den Datenschutz Geheimnisschutz

- **Akte nach Hause mitgenommen?**

Eine Strafbarkeit i.S.d. §203 StGB liegt bei Offenbarung gegenüber Dritten vor, auch wenn diese dem Familienkreis angehören....

1. Einführung in den Datenschutz Geheimnisschutz

Institut für Informationsrecht

- “Die Annahme einer mutmaßlichen Einwilligung scheidet aus, weil diese voraussetzt, dass der Geheimnisträger zweifelsfrei und erkennbar kein Interesse an der Wahrung des Geheimnisses hat oder dass er nicht rechtzeitig befragt werden kann ...„

- *BGH NJW 1992, Seite 737*

1. Einführung in den Datenschutz

•Umgang mit Daten

•§ 3a Datenvermeidung und Datensparsamkeit

•Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

•Keine Weitergabe an nicht beteiligtes Personal!

•Nur Weitergabe der notwendigen Daten!

•Trennung verschiedener Datenbereiche!

Institut für Informationsrecht

1. Einführung in den Datenschutz

•Umgang mit Daten

•Beispielsthemen:

•Der Patientenname
-an der Zimmertür
-während der Aufnahmeprozedur
-auf der Station

Zugangsmöglichkeiten
-zu Faxgeräten
-zu Unterlagen

1. Einführung in den Datenschutz

Anonymisieren (§ 3 Abs. 6 BDSG)
Daten werden so verändert, dass sie nicht mehr einer Person zugeordnet werden können.

Pseudonymisieren (§ 3 Abs. 6a BDSG)
Der Name wird durch ein anderes Identifikationsmerkmal ersetzt (Buchstaben oder Zahlenkombination, Code), um Identifizierung des Betroffenen auszuschließen oder zu erschweren.

Kernunterschied:
Bei einer Pseudonymisierung kann die Zuordnung zu einer Person wieder hergestellt werden.

Institut für Informationsrecht

1. Einführung in den Datenschutz

Ist folgender Datensatz anonym?

- Einrichtung
- Fachliche OE`s
- Pflegerische OE`s
- Aufnahmedatum
- Aufnahmezeit
- Sperrkennzeichen
- Fallart
- Anzahl Kinder
- Kz. für Komplikationen
- Datum der Entbindung
- Entlassungsdatum
- Kz. Notfall
- Kz. Auslandsfall
- Krankheitsschweregrad
- Einzugsgebiet
- Größe des Patienten
- Hauptdiagnose
- Beatmungsdauer
- Kz. für Sicherheitsverwahrung
- Geschlecht
- Fachrichtung
- Gewicht
- Postleitzahl
- DRG
- Lebensalter in Jahren
- Geburtsdatum
- Einweisender Arzt / Krankenhaus
- DRG-Typ
- Altersintervall

1. Einführung in den Datenschutz

Umgang mit Daten

§ 3a Datenvermeidung und Datensparsamkeit

Möglichst große Anonymisierung oder Pseudonymisierung!

Vorsicht vor Datenkombinationen!

Fortlaufende Nummern vergeben?

1. Einführung in den Datenschutz

Umgang mit Daten

§ 3a Datenvermeidung und Datensparsamkeit

Beispiel im Gesundheitsbereich:

Die Apothekenkasse...

Der ausgerufene Patient...

1. Einführung in den Datenschutz

Umgang mit Daten

§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Wer ist gemeint? Wer ist verantwortlich?

1. Einführung in den Datenschutz

Institut für Informationsrecht

Umgang mit Daten

§ 9 BDSG Technische und organisatorische Maßnahmen

Kontrolle von
- **Zutritt**
- **Zugang**
- **Zugriff**
- **Eingabe**
- **Auftrag**
- **Verfügbarkeit**
- **Weitergabe**

und
- **Gebot der Trennung von Daten!**

1. Einführung in den Datenschutz

Institut für Informationsrecht

Beispielsthemen:

-Datenschutz bei der Patientenaufnahme

-auf der Station

-bei Untersuchungen

1. Einführung in den Datenschutz

Institut für Informationsrecht

Beispielsthemen:

- Wann sind Patientendaten „erforderlich“?

- Ist die Fallnummer ein personenbezogenes Datum?

- Ist das Einstellen in ein konzernweites "Intranet„ eine Datenweitergabe?

- Thema Fehlendes Konzernprivileg - was bedeutet dies eigentlich für die einezlne Unternehmen (AG und AN) im Konzernverbund?

2. Datenschutz In der Medizin: Grundfragen

- **Zur Unwirksmkeit von Einwilligungen von Patienten in eine Datenübermittlung an private Verrechnungsstellen (BSG)**

- Urteil des Bundessozialgerichts vom 10.12.2008, Az: B 6 KA 37/07 R

- **Leitsatz:**
- **An einer freien Entscheidung des Betroffenen im Sinne der § 4a Abs 1 Satz 1 BDSG, § 67b Abs 2 Satz 2 SGB X fehlt es, wenn der Betroffene tatsächlich nicht die Möglichkeit hat, selbst darüber zu befinden, ob und unter welchen Bedingungen die sich auf seine Person beziehenden Angaben benutzt werden dürfen. Patienten sind - insbesondere in Notfallsituationen - zumindest subjektiv oftmals nicht frei in ihrer Entscheidung für oder gegen die Einwilligung.**

2. Datenschutz in der Medizin: Grundfragen

Auslandsdatenübermittlung im Konzern oder bei ADV?

Zulässig, wenn

- EU-Land / EWR-Land
oder
- Land mit angemessenem Datenschutzniveau oder
- Unternehmen in den USA mit „Safe Harbor“-Registrierung

Übermittlung in ein „unsicheres“ Drittland bzw. kein Safe-Harbor-Unternehmen zulässig, wenn

- Einwilligung des Arbeitnehmers (§ 4c II BDSG)
oder
- Genehmigung der Aufsichtsbehörde oder
- weitgehend unveränderte Verwendung von EU-Standardklauseln

Beispiel: Die Upper East Side Telefonanlage...

2. Datenschutz In der Medizin: Grundfragen

- *Beispiel: Daten folgen der Technik...*

- ***„1. Einführung***
- *In vielen Bereichen der Industrie, Verwaltung usw. sind Arbeitsplätze mit Computer und Telefon nicht mehr wegzudenken. Da diese Kommunikationsinfrastruktur meist durch lokale Rechnernetze und TK-Anlagen gebildet wird, liegt der Gedanke nahe, diese Komponenten miteinander zu verbinden, um bestimmte Arbeitsabläufe zu vereinfachen.“*

- *CTI steht aber nicht nur für computerunterstützte, komfortable Herstellung, Verwaltung und Beendigung von Telefonverbindungen. Mit CTI können auch Applikationen für Telefone entwickelt werden, wodurch der Funktionsumfang und das Einsatzgebiet des Endgerätes erweiterbar ist, wie z.B. elektronisches Telefonbuch (wie bei Handy), Telefon als Arbeitszeit-Erfassungsterminal.*

- *http://telecom.htwm.de/telecom/praktikum/CTI_TAPI/CTI_TAPI.htm*

2. Datenschutz In der Medizin: Grundfragen

- **IT- Sicherheit als Compliance – Risiko**

- Haftungsrisiken nicht nur für IT-Mitarbeiter, sondern über §§ 130, 30 OWiG für das Unternehmen insgesamt

- **Folge :**

- Nicht nur Präventionsverpflichtung des Unternehmens, sondern auch repressive Handlungspflichten des Unternehmens bei Verstößen

2. Datenschutz In der Medizin: Grundfragen

•Zivilrechtliche Folgen:

§ 7 BDSG Schadensersatz

•Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 823 II BGB

§116 AktG

§ 106 UrHG

Kündbarkeit von Verträgen aller Art!

2. Datenschutz In der Medizin: Grundfragen

- **Ordnungswidrigkeiten:**

- **§ 43 BDSG Bußgeldvorschriften**
-

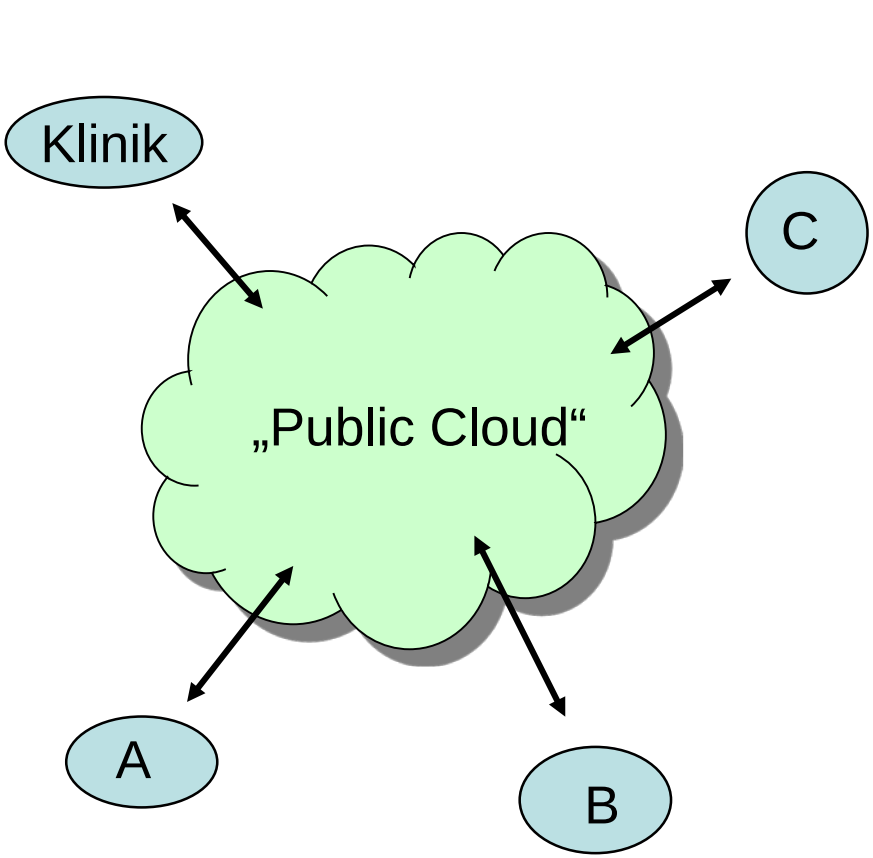
- (3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu **fünfzigtausend Euro**, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu **dreihunderttausend Euro** geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

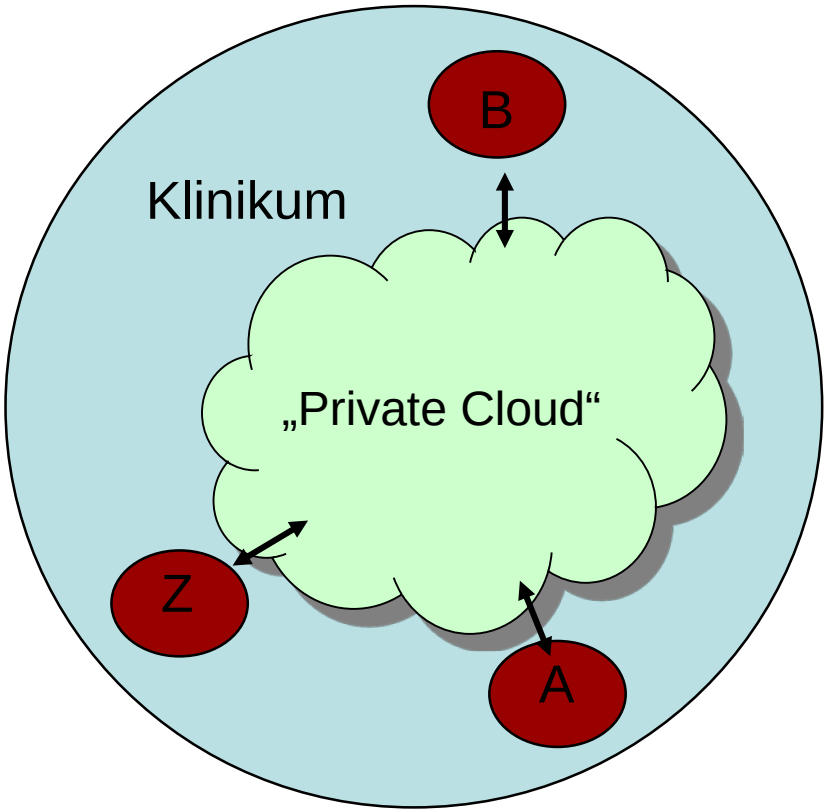
2. Datenschutz In der Medizin: Grundfragen

•**Mögliche Straftatbestände** :

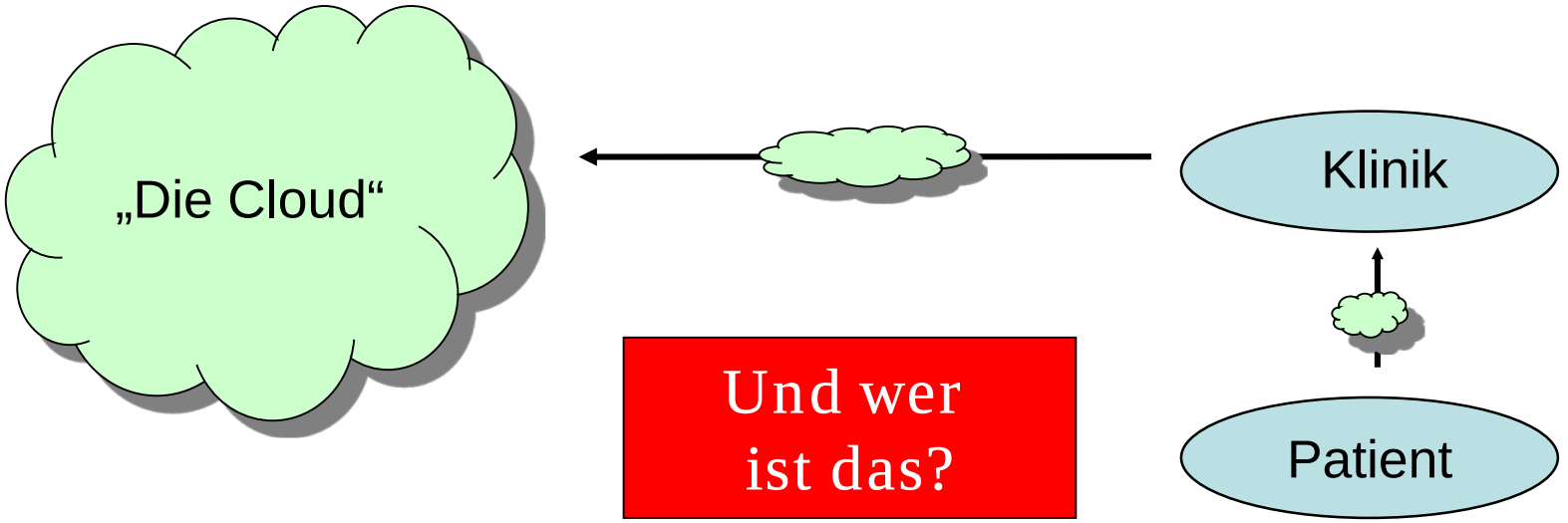
§ 203 StGB	Verletzung von Privatgeheimnissen
§ 17 UWG	Verrat von Geschäfts- und Betriebsgeheimnissen
§ 44 BDSG	
§ 202 a StGB	Ausspähen von Daten
§ 202 b StGB	Abfangen von Daten
§ 202 c StGB	Vorbereiten des Ausspähens und Abfangens von Daten
§ 269 StGB	Fälschung beweiserheblicher Daten
§ 274 StGB	Urkundenunterdrückung
§ 303 a StGB	Datenveränderung
§ 303 b StGB	Computersabotage
§ 266 StGB	Untreue (z.B. Unterlassen von Schutzmaßnahmen gegen Hacker-Angriffe)

2. Datenschutz In der Medizin: Grundfragen

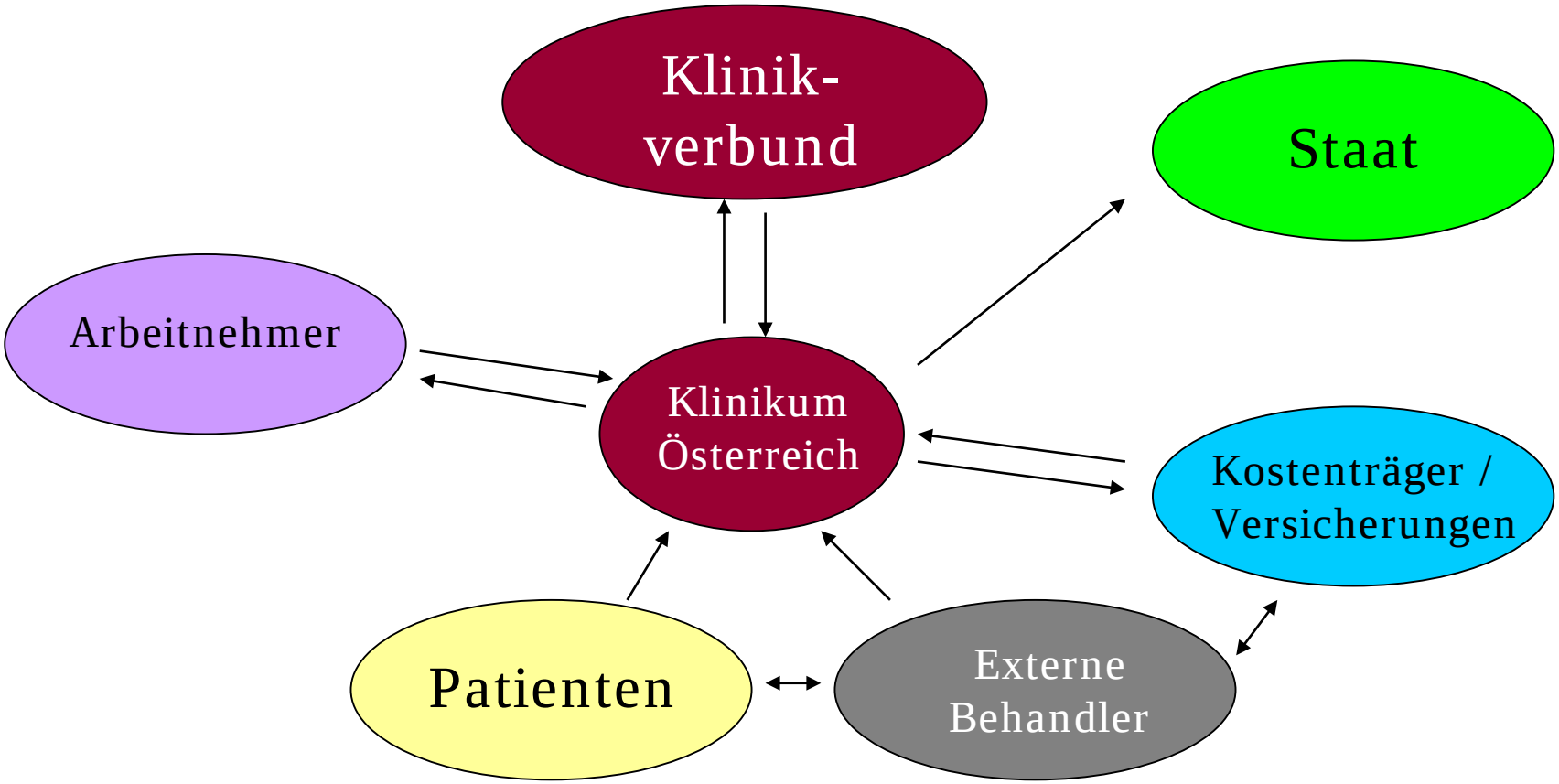




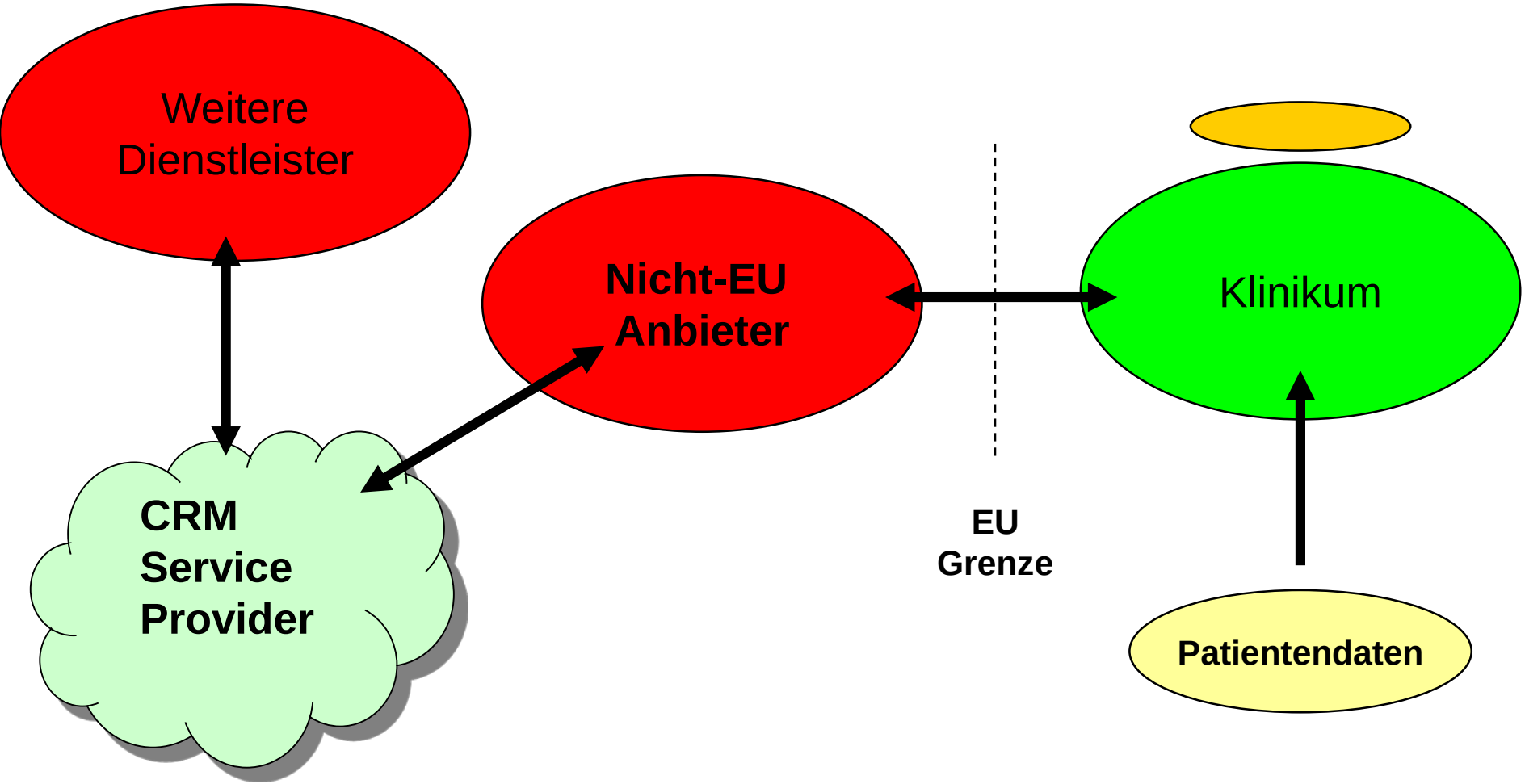
2. Datenschutz In der Medizin: Grundfragen



2. Datenschutz In der Medizin: Grundfragen



2. Datenschutz In der Medizin: Grundfragen



2. Datenschutz In der Medizin: Grundfragen

- Zulässigkeit der Weitergabe:

- Weitergabe an die Krankenhausverwaltung
- Weitergabe an externe Behandler/Labore
- Weitergabe an Kassen (SGB V)
- Weitergabe an MDK
- Weitergabe an externe IT-Dienstleister
  - ohne eigene Entscheidungsbefugnisse?
  - im Ausland?
  - innerhalb des Konzerns?

2. Datenschutz In der Medizin: Grundfragen

•Rechte der Patienten:

- Information über Erhebung
- Benachrichtigung
- Auskunft
- Einsicht in Verfahrensübersicht
- Berichtigung
- Sperrung
- Löschung

2. Datenschutz In der Medizin: Grundfragen

•Umgang mit Beschwerdefällen und Anfragen

- Kontakt mit Datenschutzbeauftragtem/r
- Dokumentation prüfen
- GGf. Hintergründe klären
- Achtung: Rechtslage unterschiedlich!
  - -Europäisches Recht
  - -Österreichisches Recht
  - -Landesrecht

Institut für Informationsrecht

Ausblick: EU-DSGVO

Anforderungen der

EU Datenschutzgrundverordnung

an medizinische Systeme und Unternehmen

I. Gründe für die Umsetzung der DS-GVO

- Anwendungsbereich:
  - Automatisierte Verarbeitung personenbezogener Daten
  - Nicht automatisierte Verarbeitung personenbezogener Daten, wenn diese in Datei gespeichert sind oder werden sollen (z.B. bei telefonischer Umfrage)
  - Niederlassungsprinzip:

    Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der EU („Niederlassungsprinzip“)
  - Marktortprinzip:

    Datenverarbeitung des Verantwortlichen oder Auftragsverarbeiters außerhalb EU mit dem Zweck, Betroffenen in EU Waren oder Dienstleistungen anzubieten

- Zeitlicher Horizont: geltendes Recht ab 25. Mai 2018

I. Gründe für die Umsetzung der DS-GVO

- Bußgeld bis zu **4 % des weltweiten Jahresumsatzes eines Unternehmens oder (für andere Datenverarbeiter) bis zu 20 Mio**. EUR, Art. 83 DS-GVO

  ⇒ Risiken aus höheren Geldbußen

  ⇒ Aber: keine Panik, der Verhältnismäßigkeitsgrundsatz gilt auch weiterhin

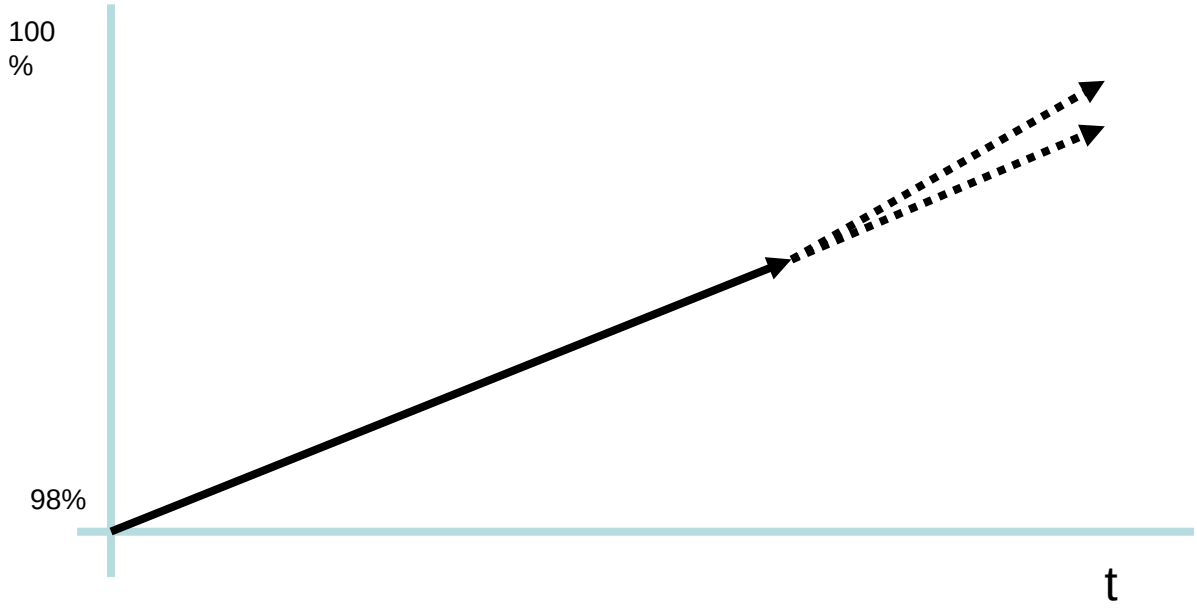
- Sonstige Maßnahmen der Aufsichtsbehörden

- **Beweisschwierigkeiten aufgrund Dokumentations- u. Nachweispflicht (Art. 24 Abs. 1 DS-GVO)**

- Zivilrechtliche Folgen (Unterlassung, Auskunft, Schadensersatz, Betroffeneninformation)

- Persönliche Haftung, Regress

I. Gründe für die Umsetzung der DS-GVO



II. Datenschutz unter der DS-GVO

- EU Datenschutz-Grundverordnung EU 2016/679 ab 25. Mai 2018 („**DS-GVO**“)

  Ca. 70 Öffnungsklauseln d. DS-GVO (=> „kompliziertes Mehrebenen-System“)
  Tipp:
  http://www.cr-online.de/blog/wp-content/uploads/2017/05/DSGVO-BDSG.htm#_Toc482877609

- Grundgesetz (Recht auf informationelle Selbstbestimmung, Rechtsprechung des Bundesverfassungsgerichts)

- Spezialgesetze, z.B.:
  - Telemediengesetz („**TMG**“)
  - Telekommunikationsgesetz („**TKG**“)
  - Gesetz gegen unlauteren Wettbewerb („**UWG**“)

II. Datenschutz unter der DS-GVO

- Neu:
  - Treu und Glauben (Verhältnismäßigkeit, „Fairness“, Wahl des mildesten Mittels)
  - Nachweisbarkeit und Dokumentation
  - Risikobasiertes Datenschutzmanagement (Risikobewertung nach Eintrittswahrscheinlichkeit und Schadenshöhe)
  - Privacy by default: Minimierung der verarbeiteten Daten durch Voreinstellung, einschließlich:
    - Menge der Daten
    - Umfang der Verarbeitung
    - Speicherfristen
    - Zugangsbeschränkungen

  - Kollision mit Big Data

II. Datenschutz unter der DS-GVO

- Nachweis der Einhaltung einer rechtmäßigen Datenverarbeitung (Art. 5 Abs. 2 DS-GVO)
- Nachweis erteilter Einwilligungen (Art. 7 Abs. 1 DS-GVO)
- Nachweis der Datenschutzorganisation, insb. angemessener technischer u. organisatorischer Maßnahmen (Art. 24 Abs. 1 DS-GVO)
- Dokumentation von Weisungen (Art. 28 Abs. 3 a DS-GVO)
- Verzeichnis der Verarbeitungstätigkeiten (Verantwortlicher und Auftragsverarbeiter, Art. 30 Abs. 1 DS-GVO)
- Dokumentation von Sicherheitsvorfällen (Art. 33 Abs. 5 DS-GVO)
- Datenschutz-Folgenabschätzungen (Art. 35 DS-GVO)

Implementierung eines Datenschutzmanagements^^

II. Datenschutz unter der DS-GVO

- Datenschutzfolgeabschätzung im medizinischen Bereich
- Durchführung, wenn die Verarbeitungsform voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge hat (auch bei bereits existierenden IT-Systemen)
- Erfordernis abhängig von Art, Umfang und Zwecken der eingesetzten Technologie, insbesondere bei:
  - Bewertung persönlicher Aspekte, inkl. Profiling
  - Verarbeitung besonderer Daten gem. Art. 9 Abs. 1 DS-GVO
  - Überwachung öffentlich zugängiger Bereiche
- Videoüberwachung, d.h. bei „systematischer und umfangreicher Überwachung“ (Art. 35 Abs. 3 DS-GVO)

II. Datenschutz unter der DS-GVO

- Aufsichtsbehörden müssen „Positivliste“ veröffentlichen
- Aufsichtsbehörden können „Negativliste“ erstellen
- => Entsprechende Veröffentlichung d. Aufsichtsbehörden beobachten
- Mindestanforderungen der Datenschutz-Folgenabschätzung:
  - Systematische Beschreibung d. Verarbeitungsvorgänge
  - Bewertung d. Notwendigkeit u. Verhältnismäßigkeit
  - Bewertung der Risiken für Rechte u. Freiheiten d. Betroffenen
  - Darstellung der zur Bewältigung der Risiken geplanten Abhilfemaßnahmen
- Konsultation der Aufsichtsbehörde, wenn ohne getroffene Datenschutzmaßnahmen ein hohes Risiko bestünde (Art. 36 DS-GVO)

II. Datenschutz unter der DS-GVO

- Bestellung erforderlich (Art. 37 Abs. 1 DS-GVO, § 38 BDSG n.F.):
  - I.d.R. mind. 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt; Verarbeitungen, die Datenschutz-Folgenabschätzung unterliegen; Geschäftsmäßige Verarbeitung personenbezogener Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung
- Erheblich erweiterter Aufgaben-und Verantwortungsbereich (Art. 39 DS-GVO):
  - Unterrichtung, (strategische) Beratung und Kontrolle des Unternehmens u. der Beschäftigten
  - Beratung der Betroffenen (Art. 38 Abs. 4 DS-GVO) und des Unternehmens
  - zur Verfügung stehen als Ansprechpartner für sowie Kooperation mit datenschutzrechtlichen Aufsichtsbehörden
- Folgen für Unternehmen:
  - Bereitstellung erforderlicher Ressourcen (sachlich, technisch, finanziell, personell)

II. Datenschutz unter der DS-GVO

- Datenschutz durch Technik

- Risikoanalyse
- technische Maßnahmen
- organisatorische Maßnahmen
- praktische Umsetzung des Zweckbindungsgrundsatzes
- technische Umsetzung des Widerspruchrechts
- elektronische Wahrnehmung von Mitteilungs- und Benachrichtigungspflichten

- Konzeption v. IT-Systemen

- Stand der Technik (ggf. Anpassung, Aktualisierung)
- Implementierungskosten
- Art und Umfang der Datenverarbeitung
- Verarbeitungszwecke
- Risikobeurteilung (Eintrittswahrscheinlichkeit u. Schadenshöhe)
- Nachweisbarkeit

II. Datenschutz unter der DS-GVO

- IT-Sicherheitsmanagement

Sicherstellung von:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Zugang zu den Daten (bzw. Wiederherstellung)

Optional: Authentizität

- Kontrollverfahren

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit
- Anforderungen an die Überwachung der Maßnahmen
- Gewährleistung der Sicherheit der Verarbeitung
- Reduzierung von Meldepflichten bspw. bei Datenpannen möglich (Art. 34 Abs. 3a DS-GVO)

II. Datenschutz unter der DS-GVO

- Abgestufte Meldepflicht von Datenpannen an Aufsichtsbehörden:
  - Meldung an Aufsichtsbehörde immer, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt
  - Benachrichtigung d. Betroffenen dagegen nur dann, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht
- Information des Betroffenen nicht (mehr) erforderlich, wenn geeignete technische und organisatorische Maßnahmen vorhanden sind, die den unbefugten Zugang auf die personenbezogenen Daten praktisch nicht ermöglichen (z.B. Verschlüsselung der Daten)
- Keine Benachrichtigung des Betroffenen, wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden und diese das hohe Risiko, das zum Zeitpunkt der Datenpanne bestand, eliminiert haben

II. Datenschutz unter der DS-GVO

- Transparente Information, Kommunikation und Modalitäten, Art. 12 DS-GVO
- Informationspflicht bei Direkterhebung, Art. 13 DS-GVO
- Informationspflicht bei indirekter Erhebung, Art. 14 DS-GVO
- Auskunftsrecht, Art. 15 DS-GVO
- Recht auf Berichtigung, Art. 16 DS-GVO,
- Recht auf Löschung,
- Recht auf „Vergessenwerden“, Art. 17 DS-GVO,.
- Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO.
- Mitteilungspflicht, Art. 19 DS-GVO
- Recht auf Datenübertragbarkeit, Art. 20 DS-GVO
- Widerspruchsrecht, Art. 21 DS-GVO
- Automatisierte Entscheidungen / Profiling, Art. 22 DS-GVODatenpannen, Art. 33, 34 DS-GVO,

III. Zulässigkeit der Verarbeitung

- Verbot mit Erlaubnisvorbehalt, d.h. jede Datenverarbeitung bedarf der Rechtfertigung
  - durch einen der Erlaubnistatbestände der DS-GVO
  - bzw. spezifischerer Vorschriften des nationalen Rechts oder des Unionsrechts
- Wesentliche Erlaubnistatbestände der DS-GVO
  - Einwilligung, Art. 6 Abs. 1 lit. a DS-GVO
  - Vertragszwecke, Art. 6 Abs. 1 lit. b DS-GVO (§ 26 BDSG n.F. f. Beschäftigtendaten)
  - Berechtigte Interessen, Art. 6 Abs. 1 lit. f DS-GVO
  - Besondere personenbezogene Daten, Art. 9 DS-GVO (§ 22 BDSG n.F.)
- Nicht geregelt in DS-GVO:
  - Spezialtatbestände (Videoüberwachung, Scoring etc.), s. aber BDSG n.F.
  - öffentlich zugängliche Daten

Minderjährige:
„frei ab 16"

Änderungen Auftragsverarbeitung

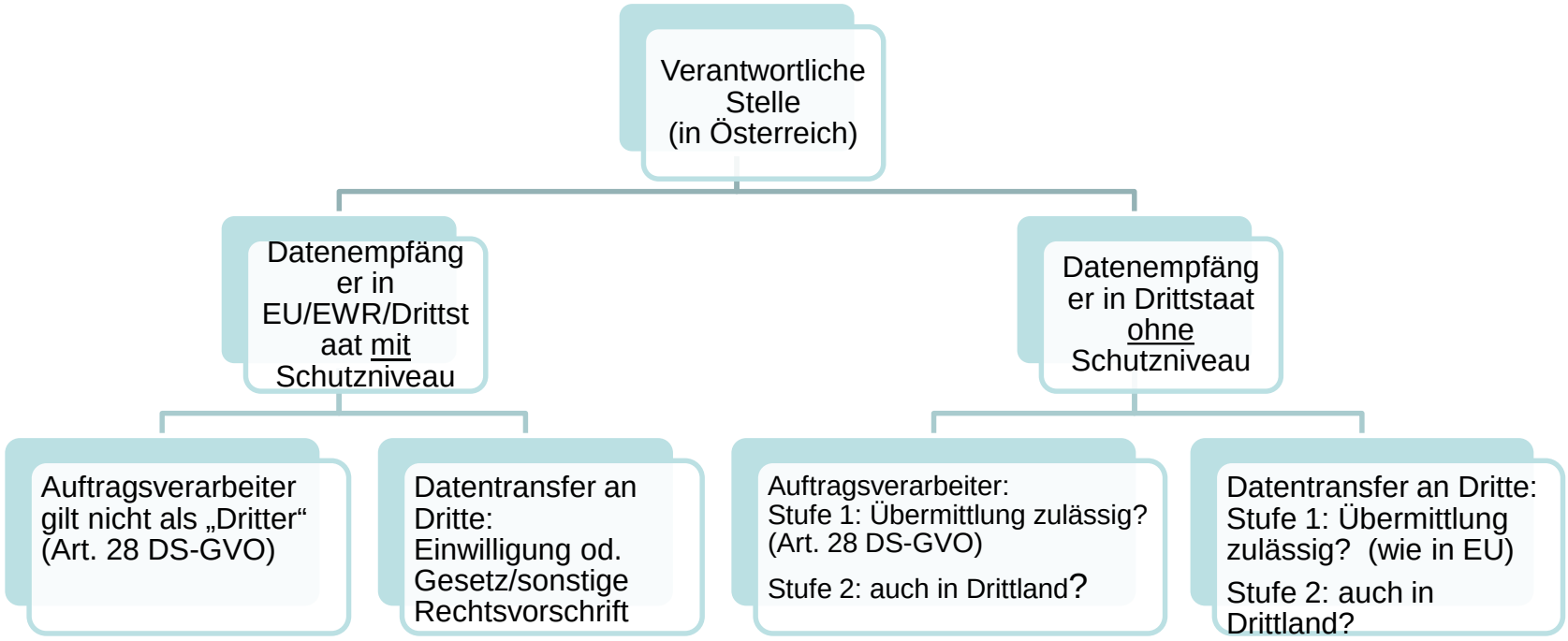
- <u>Neu:</u>

  Einsatz von Subunternehmern:

  - Zustimmungserfordernis für Einsatz von Subunternehmen und
  - Informationspflicht bei Änderungen
  - Auftragnehmer übernimmt dieselben datenschutzrechtlichen Pflichten des Auftraggebers gegenüber seinen Subunternehmen

- => Mehraufwand zur Einhaltung von Vorschriften und Sicherstellung der Nachweisbarkeit
- => Mehraufwand und erweiterte Pflichten bei Einbeziehung von Subunternehmern

III. Fallbeispiel: Auslandsdatenübertragung



III. Fallbeispiel: Auslandsdatenübertragung

- Auslandsdatentransfer:
  - Grundsatz des angemessenen Schutzniveaus bleibt bestehen
  - Keine grundsätzlichen neuen Privilegierungen
  - Art. 44ff. EU-DSGVO:
    - Art. 45 Angemessenheitsbeschluss („EU-US Privacy Shield“)
    - Art. 46 Datenübermittlung auf der Grundlage geeigneter Garantien, u.a. EU Standardvertragsklauseln
    - Art. 47 Binding Corporate Rules („BCR“)
    - Art. 49 Sonderfälle
      - Einwilligung
      - Vertragserfüllung
      - Besondere Interessen (aber Einschaltung Aufsicht)

III. Österreichische Umsetzung

- DSG 2018:
  - Nutzung verschiedener Öffnungsklauseln
  - U.a. Anpassungen bei
    - Datengeheimnis
    - Bereichsspeczifischen Regelungen
  - Art. 44ff. EU-DSGVO:
    - Art. 45 Angemessenheitsbeschluss („EU-US Privacy Shield“)
    - Art. 46 Datenübermittlung auf der Grundlage geeigneter Garantien, u.a. EU Standardvertragsklauseln
    - Art. 47 Binding Corporate Rules („BCR“)
    - Art. 49 Sonderfälle
      - Einwilligung
      - Vertragserfüllung
      - Besondere Interessen (aber Einschaltung Aufsicht)

III. Österreichische Umsetzung

- DSG 2018: Beispiel Profiling

§ 36 Abs. 2 Nr. 4 DSG-E

„Profiling“ bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

III. Österreichische Umsetzung

DSG 2018: Beispiel Profiling

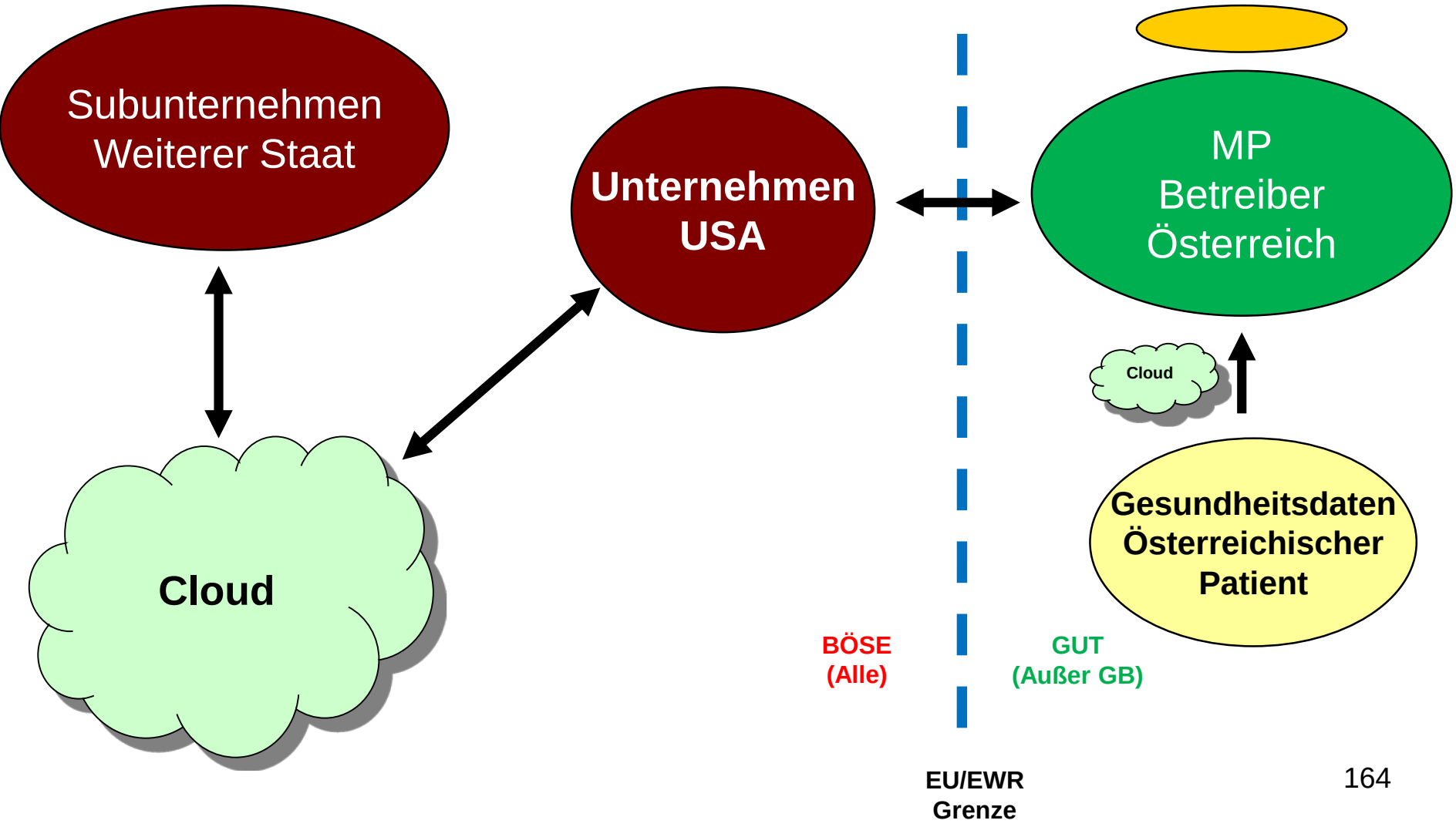
§ 41 Automatisierte Entscheidungsfindung im Einzelfall

(1) Ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidungen einschließlich Profiling, die für die betroffene Person nachteilige Rechtsfolgen haben oder sie erheblich beeinträchtigen können, sind nur zulässig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen sind.

(2) Entscheidungen nach Abs. 1 dürfen nur auf besonderen Kategorien personenbezogener Daten nach § 39 beruhen, wenn und soweit wirksame Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Entscheidungen nach Abs. 1, die zur Folge haben, dass natürliche Personen auf Grundlage von personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung diskriminiert werden, sind verboten.

BTW: Datenschutz DSG / EU-DSGVO (Datenschutzfolgeabschätzung)



IV. Ausblick: Wie schlimm wird es?

- **Typische organisatorische Themen**
  - Datenschutzmanagement / Datensicherheit / VVZ
  - Auditplanung
  - Ressource DSB
- **Typische prozessuale Themen**
  - Datenschutzfolgeabschätzung / risikobasierter Ansatz
  - Meldung von Verstößen, Schulungen
  - Einbeziehung ADV und verbundene Unternehmen
- **Typische inhaltliche Themen**
  - Datenschutzerklärung / Richtlinien / DS-Konzept
  - Einwilligungen / Betriebsvereinbarungen / Betroffenenrechte
  - ADV / Datenübertragungen im Konzern
  - Big Data / Zweckänderung und Pseudonymisierung als Option

Konsequenzen und Empfehlungen

1. Absicherung der Dateninhaberschaft muss vertraglich vereinbart werden
2. Absicherung der Datennutzung erforderlich, ggf. durch ausdrückliche Einwilligungen
3. Klärung der Gewährleistung: Wie smart darf‘s denn sein? Transparenz hinsichtlich der Existenz von Daten und Schnittstellen.
4. Verschlüsselung und Integrität
5. Anonymisierung / Pseudonymisierung

Konsequenzen und Empfehlungen

6. Datenlöschung nach Gebrauch
7. Privacy by default
8. Vorrang der Verarbeitung im Gerät (Black Box System)
9. Transparenz der Datenspeicherung im Display
10. Haftungsbegrenzungen / positive Beschreibungen, Hacking bedenken auch in der Vernetzung und bei autonomen Systemen!
11. Klärung der MDR-Auswirkungen der „Kompetenz“ des Produkts

IV. Ausblick: Wie schlimm wird es?

Unterlagen und Checklisten

- **https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html**

Danke für Ihre Aufmerksamkeit!

thomas.wilmer@h.da,de