Essentials des Datenschutzes in Zeiten der Digitalisierung

Dr. Dirk Bieresborn

Richter am Bundessozialgericht

Digitalisierung

- Von lat. *Digitus* = Finger und engl. *digit* = Ziffer) abgeleitet, Umwandeln von **analogen Werten** in **digitale Formate** und ihre Verarbeitung oder Speicherung in einem **digitaltechnischen System**
- Wird häufig alleine von der Seite des **technisch Machbaren** beleuchtet, aber regelmäßig Verarbeitung **großer Mengen von Daten**
- ->relevant für das Thema **Datenschutz**
- **->** wegen **Verkettung**
- -> zudem weitere **zwischengeschaltete Einheiten** wie **Gerätehersteller** und **Telekommunikationsunternehmen**
- **Datenschutz** dann häufig im Rahmen des Themas **„Datensicherheit“** sehr technisch gestaltet

Digitale Anwendungen im Sozialrecht:

Modernisierung der Verwaltung……

Digitale Anwendungen im Sozialrecht

- **Gesundheitstelematik (Telemedizin):** Übertragung diagnostischer oder therapeutische Daten zwischen Patient und Arzt als auch zwischen zwei Ärzten -> im Prinzip auch System der **elektronischen Gesundheitskarte (eGK)** und **elektronischen Patientenakte (ePA**)
- Derzeit zu unterscheiden: **freiwillige** und **Pflichtanwendungen**,

Digitale Anwendungen

- **Telenursing**: Applikationen für Arzt, Pflegende, Gepflegte und deren Angehörige: → Case Management, Reha-Maßnahmen, Tele-Visiten z.B. zur Wundversorgung
- **Ambient Assisted Living (AAL)**: technische und personale Unterstützungsmaßnahmen im häuslichen Bereich einer pflegeunterstützungsbedürftigen Person.

- -> **automatisierte Bewegungs-**
- **meldesysteme**

- → **Roboter** als schlichte **Mobilitätshilfen** und **Assistenzroboter** zur physischen Alltagsunterstützung, in denen Navigationsfähigkeiten mit anspruchsvollen Manipulationstätigkeiten kombiniert werden
- → setzen **physische Interaktion**

mit Gegenständen (**Internet of the Things**)

und Personen voraus

- → Fragen **künstlicher Intelligen**z (KI)

und des **Maschine Learning** (ML)

- **Grundlagen, Systematik Datenschutz**

„Recht auf Datenschutz“

- **Subjektives Recht**, das unmittelbar aus Verfassung als **Recht auf informationelle Selbstbestimmung (Art 2 Abs 1 iVm. Art. 1 Abs 1 GG = APR)** resultiert.
- Es umfasst: **Recht des Einzelnen**, grundsätzlich **selbst zu entscheiden**, wann und innerhalb welcher Grenzen **persönliche Lebenssachverhalte offenbart** werden (BVerGE 65, 1, 42)
- Eingriffsvorbehalt (Art 2 Abs 1 GG): **Verhältnismäßigkeit**
- Schutz beginnt bereits auf der Stufe der Persönlichkeitsgefährdung im **Vorfeld konkreter Bedrohungen!** (BVerfG 115, 320, 340) **->Datensicherheit!**

Entwicklung EU-Recht

- **1995: Datenschutzrichtlinie 95/46/EG (DSRL)**
- **2000: Art 8 EUChGr:**
- *1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*
- *(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden……*
- **EU- Datenschutz-Grundverordnung** (als **VO (EU) 2016/679** v **27.4.2016** verabschiedet (Abl.L.119).
- **Gilt** in den Mitgliedstaaten seit **25.5.2018 ohne Umsetzungsakt** (Art 99 Abs 2 DSGVO)

Systematik DSGVO/BDSG/SGB I/X

- **Ziel der DSGVO:** Festlegung eines **allgemeinen Datenschutz-Rechtsrahmens der EU** *(„one size fits all…*“) ohne Unterscheidung zwischen **öffentlichen** und **privaten Datenverarbeitern**,
- Widersprechende nationale Regelungen sind **unanwendbar (*Vorrang des Europarechts*)!**
- Da nur **Grund**verordnung: → **Regelungsspielräume** zur **Präzisierung und Konkretisierung,** → **Öffnungsklauseln** für **bereichsspezifische Regelungen.** → Dies nun Funktion von **BDSG/SGB I/X** u.a., aber auch **Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)** (seit 1.12.2021) und **Telemediengesetz (TMG)**
- Wegen **Wiederholungsverbot -> Mehrebenensystem!**
- **ePrivacy-VO** noch nicht in Kraft

Was sind personenbezogene Daten?

- **Art. 4 Nr 1 DSGVO:** ***alle Informationen****, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die* ***direkt o. indirekt****, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,* ***identifiziert*** *werden kann.*
- Keine Definition mehr der **Anonymisierung** (EG 27)

Rechtsgrundlagen für Datenverarbeitung

- **Art 6 Abs 1 DSGVO** enthält **6 Unterfälle:**
- Einige bilden **unmittelbare Rechtsgrundlagen** (kein Handeln des nationalen Gesetzgebers erforderlich):
  - Buchst a) ***Einwilligung***,
  - Buchst b) ***Vertrag***
  - Buchst f) ***Wahrnehmung berechtigter Interessen*** **(nur für Private!)**
- Ansonsten Rechtsgrundlagen (auch für **öffentliche Stellen):**
  - Buchst. c) und e): ***Erfüllung rechtlicher Verpflichtung*** *bzw. in* ***Ausübung öffentlicher Gewalt,***
  - → bedürfen Konkretisierung durch **Mitgliedstaaten** → Nationaler Gesetzgeber bestimmt, was **öffentliche Aufgaben** sind (Art 20 GG)
  - **->** z.B. **§§ 22 ff BDSG** , **§§ 67a, 67c, 67d SGB X** (vgl. Art 6 Abs 3 und Abs 2 VO).

Besondere Daten-Kategorien

- **Art. 9 Abs 1 DS-GVO verbietet** Verarbeitung Daten über
  - rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit
  - genetische, biometrischen Daten zur eindeutigen Identifizierung einer Person, **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung.

Es sei denn, es besteht **Öffnungstatbestand nach Art 9 Abs 2 DSGVO**.

=> Buchst a) *(ausdrückliche Einwilligung)*

⇒ Buchst b): *Soziale Sicherheit*:=> §§ 67a ff SGB X; weitere Einschränkung gem Art 9 Abs 4 iVm § 67 b Abs 2 SGB X; *Arbeitsrecht* => § 26 Abs 3 BDSG

Sozialdaten (§ 67 SGB X)

- **Bereichsspezifische Konkretisierung** nach deutschem Recht.
- Daten müssen von einer der in § 35 SGB I **genannten Stelle**
  - im Hinblick auf **deren Aufgaben nach dem SGB**
  - **verarbeitet** werden
- **§ 78 SGB X**: Die **Dritten** haben die Daten in **demselben Umfang geheim** zu halten wie die **in § 35 SGB** I genannten Stellen (= verlängerter Datenschutz).
- Nicht zu verwechseln mit **besonderen Kategorien** von Daten nach Art 9 DSGVO
- **=>** z.B. **Gesundheitsdaten** sind **häufig**, aber **nicht immer** auch Sozialdaten!

- **Grundprinzipien in Bezug auf Digitalisierte Datenverarbeitung**

Grundprinzipien DS-GVO (Art 5 DS-GVO)

- **Rechtmäßigkeit, Treu und Glauben, Transparenz, Richtigkeit**
- **Rechenschaftspflicht des Verantwortlichen (*accountability*)**
- **Zweckbindung,**
- **Datenvermeidung, -sparsamkeit, Speicherbegrenzung**
- **Integrität und Vertraulichkeit**
- ***Privacy by design* and *privacy by default* (Art 25 DS-GVO)**
- -> Von vornherein muss möglichst vermieden werden, dass Daten zur Kenntnis Unbefugter gelangen –> **Need-to-Know-Prinzip!**

Aber auch: **Schutz der Grundfreiheiten!** (Art 1 Abs 2 DSGVO)

Datenminimierung/-sparsamkeit

- Daten müssen dem Zweck **angemessen** und **erheblich** sowie auf das für die Zwecke der Verarbeitung **notwendige Maß** beschränkt sein« (Art 5 Abs 1 Buchst c) DS-GVO).
- Daten müssen „*in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden,* ***erforderlich*** *ist*“ (Art. 5 Abs. 1 Buchst. e DS-GVO)
- -> Problem bei **Robotern, KI, Maschine-Learning**…..Was ist erforderlich?
- -> Datensparsamkeit lässt sich auch dadurch realisieren, dass schon bei der **Erhebung** Rohdaten umgehend **aggregiert** und nur diese gespeichert oder weitergegeben werden.

Zweckbindungsgrundsatz

- Auch **Art 5 EU-DSGVO** verlangt **Festlegung des Verarbeitungszwecks**.
- Wenn zu **anderem als zum Erhebungszweck** genutzt
- -> *zweckändernde Weiterverarbeitung*
- Nach **Art 6 Abs 4 DSGVO** zulässig bei
  - - Vorliegen einer ***Einwilligung,***
  - *- oder* ***einer Rechtsvorschrift der Union oder der Mitgliedstaaten***
- Bei **Fehlen dieser Bedingungen** weiterer **Ausnahmetatbestand: Verantwortlicher erhält Prüfungskompetenz zur Feststellung der Zweckkompatibilität**: 5 Positiv- Kriterien wie *Art, Verbindung, Zusammenhang der Daten*, *Folgenabschätzung*.
- Kann dies durch **nationale Gesetze** verhindert werden?
- Was ist, wenn **Forschungsinstitut** Gesundheitsdaten zu **anderen Zwecken** verwendet/verkauft für -> **Kosmetikindustrie…..???**

Normen, die Digitalisierung betreffen

- Nur wenige Normen betreffen Digitalisierung, und wenn weniger datenschutzrechtliche Belange:
- **§ 33a SGB V, § 67 SGB V, § 75 b SGB V**
- **§ 39a SGB XI, § 40a SGB XI; und 40b SGB XI.**
- **§ 139e Abs 9 SGB V** ermächtigt Exekutive zur verbindlichen Regelung datenschutzrechtlichen Anforderungen
- Am präzisesten: **§ 291a SGB V (eGK), § 341 SGB V ff (ePA),** getrennt nach Pflichtangaben und freiwilligen Angaben

Technologieneutralität

- Die DS-GVO versteht sich selbst als **technologieneutral** (ErwG 15).
- → Sie beansprucht **nicht**, konkrete technische Entwicklungen zu steuern,
- → sondern Regeln vorzugeben, die sich durch eine **möglichst hohe Abstraktion gegenüber Technik** auszeichnen.
- → keine **spezifischen Erlaubnistatbestände** für den Umgang mit Daten bei
  - → Cloud-Computing,
  - → Big-Data-Analysen
  - → für sensorische Umgebungen
  - → autonome Roboter, KI, Algorithmen…
- Offen für **neue Entwicklungen!**

- **Die Einwilligung**

Einwilligung

- Nur erforderlich, wenn **keine andere Rechtsgrundlage,**
- **-> d.h. hier, wenn digitale Anwendungen nicht aufgrund eines Gesetzes erfolgt!**
- **Art 4 Nr 11/Art 7 DSGVO** verlangen
  - **freiwillige**
  - **Willensbekundung**
  - in **informierter** Weise
  - auch über **jederzeitiges Widerrufsrecht!**
  - **Nachweismöglichkeit** des Verantwortlichen.
- **§ 67b Abs 1 SGB X**: *Schriftlich* oder *elektronisch*
  - -> Wegen **Datensicherheit** eMail nur restriktiv möglich

Aktive Willensbekundung

- Heißt, dass **aktiv zugestimmt** werden muss, durch zumindest eindeutige **bestätigende Handlung** (EuGH vom 1.10.2019 - *C-673/17 (Planet49)* zu RL 2002/58 und 95/46/EG)
- -> **kein Opt-Out** sondern **Opt-In!** *(So auch BGH zu § 15 Abs 3 Telemediengesetz (TMG) vom 28.5.2020 – I ZR 7/16 – juris*.
- Dies beachten nicht
  - **SVR-Gutachten**
  - sowie **Koalitionsvertrag**!
- Zudem ist auch bei Einwilligung **Verhältnismäßigkeitsprinzip** umzusetzen
- -> **feingranulares Zugriffsmanagement**!

Erwägungsgrund 43

- **Konflikt mit Mitwirkungspflichten (§§ 60 ff SGB I) wegen Erwägungsgrund 43:**
- Einwilligung keine gültige Rechtsgrundlage bei **klarem Ungleichgewicht**, *„insbesondere wenn es sich bei dem* ***Verantwortlichen um eine Behörde*** *handelt, und es deshalb* ***in Anbetracht aller Umstände*** *in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung* ***freiwillig*** *abgegeben wurde...“*
- Bei **Einsatz komplizierter Technologie** fraglich, ob Betroffener versteht, was mit seinen Daten passiert!
- Gilt insbesondere im Bereich **Pflege** (Stichwort **„Demenz“)**

- Ärztliche Schweigepflicht

Ärztliche Schweigepflicht

- Besteht n. **§ 1 Abs 2 BDSG/§ 35 Abs 2a SGB I** neben (Sozial-)datenschutz
- → **Zwei-Schranken-Theorie.**
- **Standesrechtliche Rechtsgrundlage:** § 9 Musterberufsordnung
  Strafrecht: § 203 Abs 1 Nr. 1 und Nr. 2 StGB
- Unter Strafe gestellt ist nur **unbefugtes Offenbaren=> Befugnis** aus:
  - **Einwilligung** (auch mutmaßlicher!)
  - **Gesetz** (z.B. § 138 StGB, dann sogar Pflicht!)
- Im Übrigen: **Rechtfertigendem Notstand** (§ 34 StGB)
    - Verteidigung des Arztes
    - Schutz höherwertiger Rechtsgüter
- **-** > Nicht jede **gesetzliche Übermittlungsbefugnis** enthält Befugnis zur **Verarbeitung ärztlicher Daten**! => § 76 SGB X, vgl. § 203 SGB VII, § 274 ff SGB V

- **Der (datenschutzrechtlich) Verantwortliche**

Wer ist Verantwortlicher?

- Frage ist **wichtig**
  - für **Betroffenenrechte**
  - **Belehrungspflichten** bei bestimmten Übermittlungen
- Art 4 Nr 7 DSGVO:
  - …„*Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die* ***allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet****; …..*
- Art 4 Nr 8:…
  - “**Auftragsverarbeiter**“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet.

Auftragsverarbeitung

- Bedingungen der AV werden in Art. 27, 28, 29 DSGVO normiert. Ansonsten keine **Definition!**
- **§ 80 SGB X** regelt nicht das „**Wie**“, sondern das „**Ob**“ der Auftragsverarbeitung bei **Sozialdaten**
- Auch hier Auftragsverarbeitung nach wie nicht definiert:
  - Kein **eigenes Interesse** an Daten
  - Keine **Funktionsübertragung**
  - H.M.: **Strikte Weisungsgebundenheit** bzgl Datenumgang
- Abgrenzung zwischen **Verantwortlichen**, die über **„*Zweck und Mittel der Datenverarbeitung*“** entscheiden, und **Auftragsverarbeitern** mehr als streitig.

Verantwortlicher oder Auftragsverarbeiter?

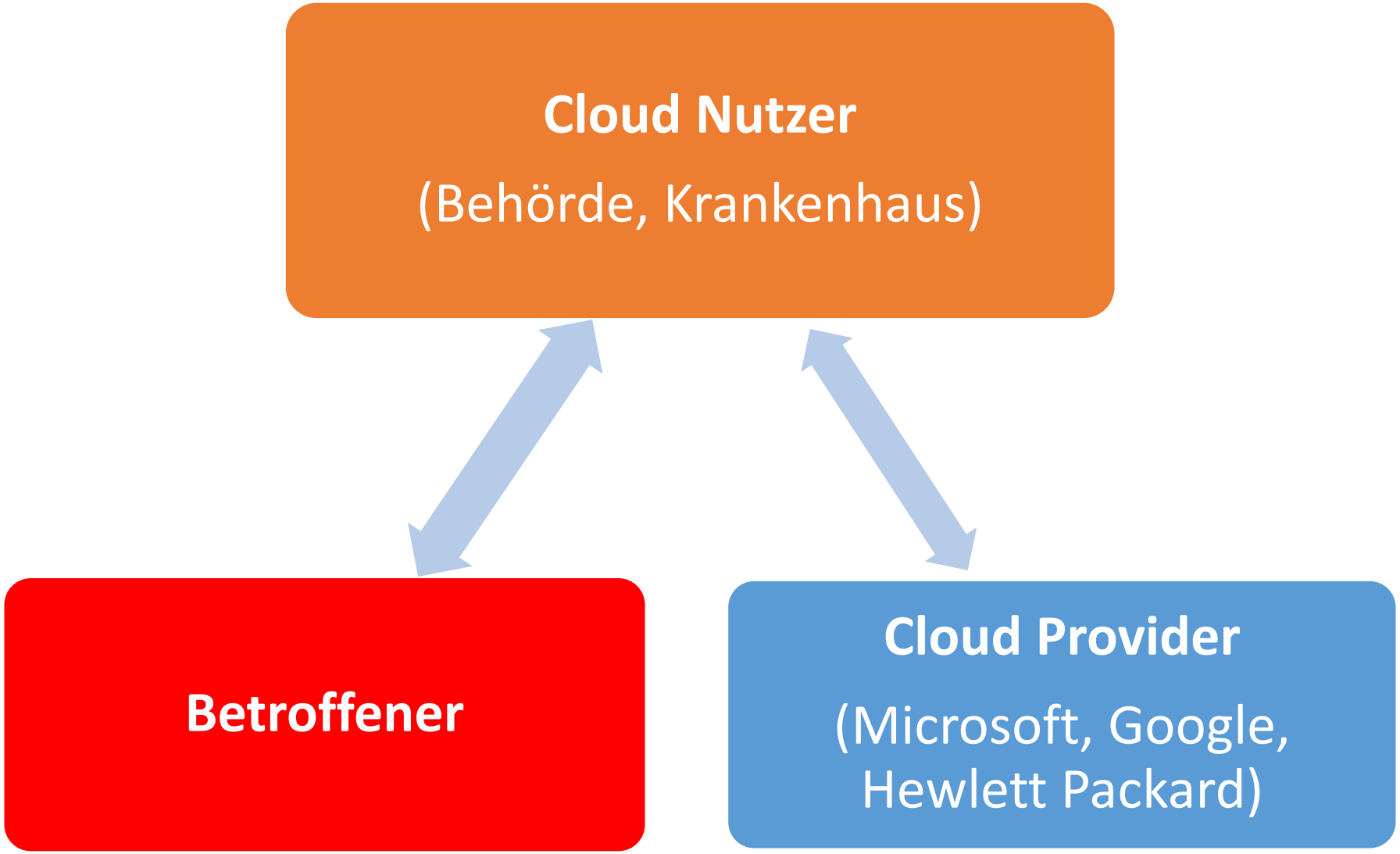
- Leistungsträger (§ 67 Abs 4 SGB X)
- Gerätehersteller?
- Gerätebetreiber?
- Arzt, Pflegedienst?
- Telekommunikationsanbieter? – (*Location Based Services*)
- Internetprovider?
- => Es spricht viel dafür, dass diese Player als **„Gemeinsam Verantwortliche“** agieren und eine **„Flucht in die Auftragsverarbeitung“** nicht möglich sein wird.
- Es genügt auch **sukzessives Handeln** (EuGH, Urt. v. 29.7.2019 - C-40/17 („Fashion ID)

- **Nutzung cloudbasierter Anwendungen**

Cloud Computing

- Form des **IT-Outsourcing**: Ressourcen werden im Hinblick auf Software und/oder Hardware dezentral über Internet zur Verfügung gestellt
- **Ziel:** IT Dienstleistungen **dynamisch und skalierbar** nutzen zu können, zu unterscheiden: **Private Cloud, Public Cloud, Government Cloud, Hybrid Cloud**
- Cloud Computing gilt als **Auftragsverarbeitung** iSv Art 28 ff DS-GVO/§ 80 SGB X -> Cloud-Provider ist **nicht Dritter** und es findet **keine Übermittlung** statt.

Rechtliche Beziehungen beim Cloud Computing



Cloud Computing

- Auftragsverarbeitung darf – wie bisher – **nur innerhalb der EU/EFTA** und – neu - **in Drittsaaten mit Angemessenheitsbeschluss** erfolgen (Art 49 DS-GVO, § 80 Abs 2 SGB X)
- Gem § 80 Abs 2 SGB X darf Auftragsverarbeitung, der nicht das „Wie“ sondern „Ob“ beschreibt, auch in „**White-List-Countries“ erfolgen.**

Übermittlung in USA

- Zunächst wurden USA unter Voraussetzung von ***Privacy Shield*** in *White-List* der Kommission aufgenommen.
- Der EuGH hat inzwischen auch diesen Beschluss der Kommission für unwirksam erklärt, weil insbesondere der **Ombudsmechanismus** nicht mit Rechtsschutz nach Art 46 GRCh korrespondiert (Urteil des EuGH vom 16.07.2020 - C-311/18 ("Schrems II").
- Daher nur zulässig bei **besonders vereinbarten Standardvertragsklauseln**

- **Künstliche Intelligenz/ Maschine Learning**

Verbot automatisierter Entscheidungen – Art 22 DSGVO

- Zweck des **Art. 22 Abs. 1 DSGVO** ist es, Betroffene nicht zum **bloßen Objekt künstlicher Intelligenz** – z.B. **Algorithmen** - zu machen.
- Unter einer automatisierten Entscheidung wird eine Computerentscheidung **ohne menschliche Einflussnahme** verstanden.
- => Nicht wenn automatisiertes System eine **von Menschen vorfestgelegte Entscheidung** trifft *(Beispiel: Menge der Infusion hängt von der automatisierten Feststellung bestimmter Blutwerte ab)*
- Erfolgt jedoch **automatisiert** keine vorfestgelegte überschaubare **„Wenn-dann-Entscheidung“**, sondern ein komplexer, für den Betroffenen nicht mehr überschaubarer Entscheidungsprozess, dann findet Art. 22 DS-GVO unabhängig von der Wertigkeit und Fehleranfälligkeit der Entscheidung Anwendung.
- Dies ist stets bei **KI** der Fall!

- **Big or Small Data….?**

Digitale Verarbeitung bedeutet häufig Big Data

- = Analyse großer Datenmengen aus vielfältigen Quellen in hoher Geschwindigkeit mit dem Ziel, wirtschaftlichen Nutzen zu erzeugen
- *„New Oil“* der Wirtschaft
- Interessant auch für Sozialleistungsträger, aber nicht nur aus wirtschaftlichen Gründen (*„Fitness-Apps“)*
- Sondern auch um Leistungen zu verbessern

Elektronische Gesundheitskarte/elektronische Patientenakte in der Rechtsprechung

- **Verhältnismäßiger Eingriff** in Recht auf informationelle Selbstbestimmung (*BSG vom 18.11.2014 – B 1 KR 35/13; BSG vom 20.1.2021-B 1 KR 7/20 R, B 1 KR 15/20 R*) bei **Pflichtdaten**
- Gilt auch im Hinblick auf **Datensicherheit** wegen genutzter **Telematikinfrastruktur**
- Derzeit aber nur **Lichtbild, Geschlecht und Zuzahlungsstatus**, § 291 Abs 2 S 1 Nr 4 und 8 SGB V nF : „*Small Data*“, über freiwillige Daten keine Entscheidung des BSG
- Zukünftig aber **Diagnosen, Medikamente als Pflichtangaben….????**

eHealth

Chancen

- Schnellere Hilfe bei Notfällen
- Schutz vor Medikamenten-Missbrauch
- Rechtzeitiges Erkennen und Eindämmen von Epidemien
- Effektivere Forschung durch breitere Erkenntnisquellen (z.B. Krebs)

Risiken

- „Gläserner“ Patient
- Kaum Schutz vor Verlust oder „Hacking“
- Diskriminierungsgefahr bei Bekanntwerden intimer Gesundheitsdaten (z.B.HiV)
- Bei Genom-Daten Gefahr der Diskriminierung nachfolgender Generationen

Fazit

- Digitale Datenverarbeitung kann viele **Vorteile** bewirken
- Aber birgt auch **datenschutzrechtliche Risiken**
- **Rechtsgrundlage** Gesetz oder (ausdrückliche) Einwilligung
- Aber keine Vermischung durch **Opt-Out**
- Klare **Begrenzung zweckändernder Datenverarbeitung**
- Bestmöglicher Schutz vor **Datenabfluss**
- Ungeklärter Umgang mit **KI**
- Erforderlich ist **intensiver Diskurs** in der Gesellschaft, wie weit man **Technik** nutzen möchte trotz immer bestehender **Restrisiken**