

# **Aktuelle Herausforderungen des Sozialstaates:**

## **Sozialdatenschutz**

Prof. Dr. Dirk Bieresborn

Vorsitzender Richter am  
Bundessozialgericht

Datenschutzbeauftragter

# Stichworte (statt Gliederung)

- Basics (Sozial-)Datenschutz
- Sozialstaatsreform
  - Once-Only-Prinzip/Frontoffice
  - Direkterhebung
  - Abrufverfahren
- Datenschutz und Digitalisierung?
  - Einwilligung oder Gesetz
  - KI
  - Auftragsverarbeitung
  - Der „Digital Omnibus“ und die DSGVO

# „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.
- -> **Recht des Einzelnen**, grunds. **selbst zu entscheiden**, wann und innerhalb welcher Grenzen **persönliche Lebenssachverhalte offenbart** werden (BVerfGE 65, 1, 42)
- Eingriffsvorbehalt (Art 2 Abs 1 GG):
- -> **Verhältnismäßigkeit**
- Schutz beginnt bei Persönlichkeitsgefährdung im **Vorfeld konkreter Bedrohungen!** (BVerfG 115, 320, 340)
- -> **Datensicherheit!**

# Systematik DS-GVO (seit Mai 2018)

- **Ziel der DS-GVO:** 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 **Grundverordnung**:
- → **Regelungsspielräume** zur **Präzisierung** und **Konkretisierung**,
- → **Öffnungsklauseln** für **bereichsspezifische Regelungen**.
- → **BDSG/SGB I/X**

# Grundprinzipien der DS-GVO

---

- **Rechtmäßigkeit der Datenverarbeitung** (nicht nur „Ob“, sondern auch „Wie“!)
  - → **Rechtsgrundlage** erforderlich (zB Gesetz, Einwilligung)
- **Datenvermeidung, -sparsamkeit; Speicherbegrenzung**
  - → Verhältnismäßigkeitsprinzip
- **Zweckbindung**
  - → Datenverarbeitung zu **anderem als zum Erhebungszweck** nur **eingeschränkt** zulässig
- **Privacy by design sowie by default**
  - → bei **digitaler Verarbeitung** durch **konsequentes Rechtekonzept** (*Need to know-Prinzip*) leichter umsetzbar!

Aber auch: **Schutz der Grundfreiheiten!** (Art 1 Abs 2 DSGVO) → Damit auch **Schutz der Wettbewerbsfreiheit**, s zur **Forschungsfreiheit** Art 5 Abs 1 Buchst b) DSGVO

# Sozialdaten (§ 67 SGB X)

- Deutsches Recht unterscheidet
  - „normale“ Daten (geregelt im BDSG und LDSG'en, TDDDSG usw )
  - „**Sozialdaten**“ (SGB I/X)
    - -> **Bereichsspezifische Konkretisierung** nach deutschem Recht
    - -> typisierend betrachtet erhöhter **Schutzbedarf**, da **näher an Privatsphäre** heranreichen
    - = Daten, die von einer in **§ 35 SGB I** genannten **Stelle** (idR Sozialleistungsträger
    - im Hinblick auf **deren Aufgaben nach dem SGB** verarbeitet werden
- **Nicht zu verwechseln mit besonderen Kategorien von Daten nach Art 9 DSGVO**
- => z.B. Gesundheitsdaten sind häufig, aber nicht immer auch Sozialdaten!

# Front-Office/ One-Stop-Shop/ Once-Only-Prinzip



Sowohl bei **Datenerhebung** als auch – **speicherung** ist **Verhältnismäßigkeitsprinzip** zu beachten



Welche Daten werden gebraucht?



Wie lange werden diese gespeichert?



Erhebungs-/Speicherzweck und Dauer muss Gesetzgeber vorgeben, ansonsten **unzulässige Datenvorratserhebung!**



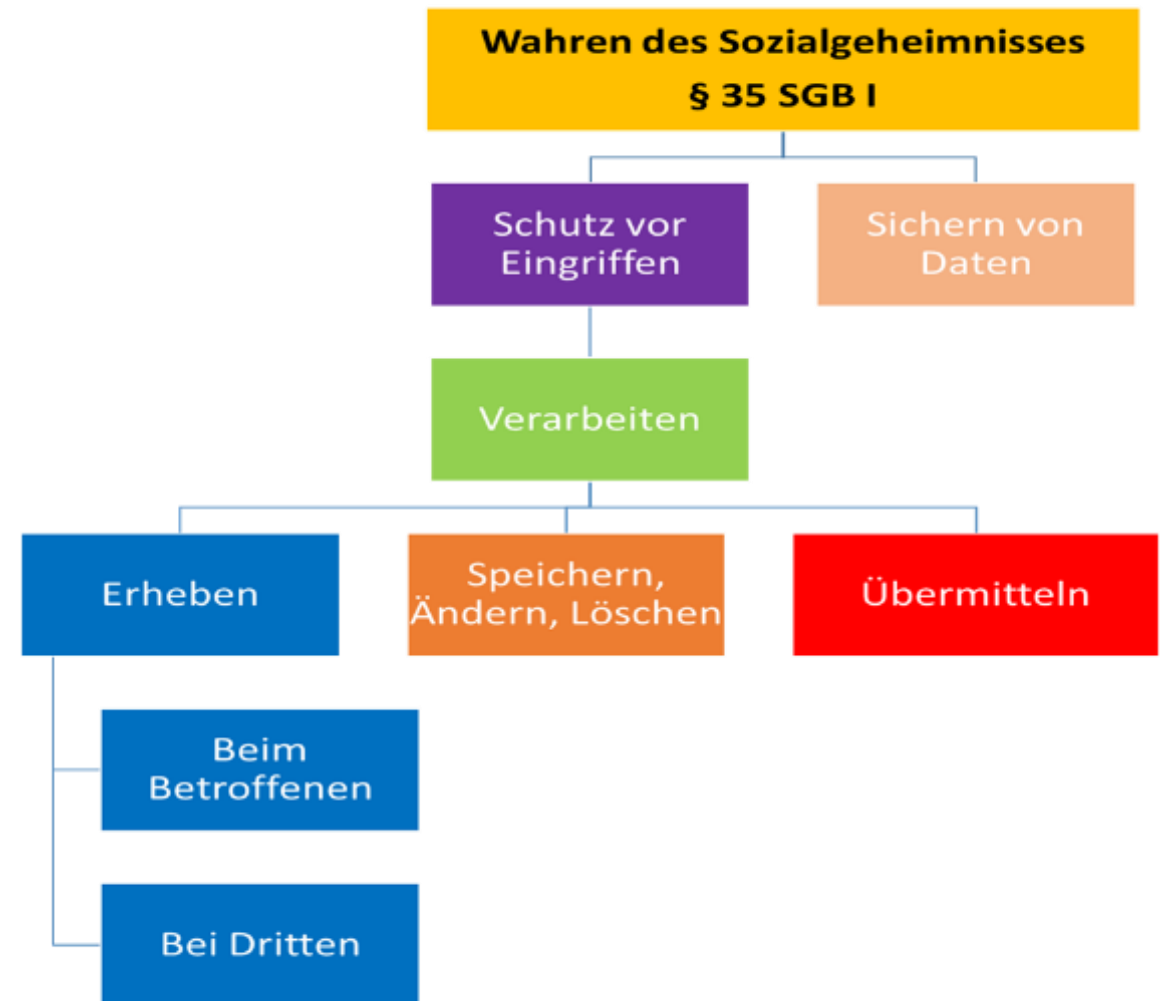
ELENA-Verfahren....



Art 17 DS-GVO:→ „Recht auf Vergessenwerden“

# Direkterhebungsgrundsatz

- § 67a Abs 2 SGB X :
  - Erhebung grundsätzlich **beim Betroffenen**
  - Erhebung bei Dritten grundsätzlich nur **unter Mitwirkung des Betroffenen**
  - Erhebung bei **Dritten ohne Mitwirkung** des Betroffenen nur **in Ausnahmefällen**, wenn gesetzlich vorgesehen (s. § 60 SGB II, § 117 SGB XII) oder bei **besonderer Eilbedürftigkeit** und **keine überwiegenden schutzwürdigen Interessen entgegenstehen** (BSG v. 25.1.2012 – B 14 AS 65/11 R)





# Sozialstaatskommission

- „Vereinfachung des Sozialdatenschutzes“
- → **Abschaffung des Direkterhebungsgrundsatzes?**
- → Setzt **DSGVO** nicht zwingend voraus, nur unterschiedliche Informationspflichten (Art 13 und 14 DSGVO)
- → Ausfluss **Verhältnismäßigkeitsprinzip**: Erhebung bei Dritten immer **auch Übermittlung** des Erhebungszwecks!
- → gegenüber **anderen Behörden** unproblematisch, ohnehin großzügige **Übermittlungsnormen** (§ 69 Abs 1 SGB X, § 76 SGB X), auch zur **zweckändernden Datenverarbeitung** (§ 67c SGB X)
- **Vorsicht bei Privaten!**

# Automatisierte Abrufverfahren?

---

- Existierende Rechtsgrundlagen:
  - **§ 79 SGB X**
  - **§ 67f SGB X** ermöglicht Behörden, vorhandene synchrone Daten auf Veranlassung der betroffenen Person **einfach und sicher auszutauschen**.
  - Zur Ermittlung und Prüfung der **Anrechnung des Einkommens** nach **§ 97a SGB VI** erfolgt der dafür notwendige Datenaustausch zwischen den **Trägern RV** und den **Finanzbehörden** bereits automatisiert (**§ 151b SGB VI**).
- Nach wie vor **Übermittlung**
  - → Grundsätzlich **geteilte Verantwortlichkeit** zwischen der übermittelnden Stelle und der abrufenden Stelle (§ 67d Abs 1 SGB X).
  - Verantwortung für die Zulässigkeit der **einzelnen Abrufe** werden der **abrufenden Stelle** auferlegt (§ 79 Abs 4 Satz 1 SGB X), weil diese ohne Mitwirkung der verantwortlichen Stelle agieren kann.
  - Damit birgt die Einrichtung automatisierter Abrufverfahren **größere Risiken**, da nur **eine Kontrollinstanz** besteht,
  - → **erhöhte Anforderungen an die Verhältnismäßigkeitsprüfung** bei der Schaffung entsprechender Rechtsgrundlagen zu stellen sind.

# Digitalisierung

- ist relevant für das Thema **Datenschutz**
  - → wegen **großer Mengen von Daten**
  - → wegen **Verkettung**
  - → wegen großer **Geschwindigkeit** der Verarbeitung
- Datenschutz dann häufig im Rahmen des Themas „**Datensicherheit**“ sehr **technisch** gestaltet
- Herausforderung **einheitlicher IT-Systeme/Software-Lösungen** im Föderalismus
  - Grundgesetzänderung?
  - Staatsverträge? zB **NOOTS** (= *Nationale Once-Only-Technical-System* zur Registermodernisierung)

# Technologieneutralität

- Die DS-GVO versteht sich selbst als **technologieneutral** (ErwG 15).
  - → beansprucht **nicht**, konkrete **technische Entwicklungen** zu steuern,
  - → keine **spezifischen Erlaubnistatbestände** für den Umgang mit Daten bei
    - → **Cloud-Computing**,
    - → **Big-Data-Analysen**
    - → **autonome Roboter, KI, Algorithmen...**
- Offen für **neue Entwicklungen! Risikobasierter Ansatz!**
- BSG vom 20.1.2021 - B 1 KR 7/20 R: Es gibt **keine absolute Datensicherheit!**  
Sicherheitsmaßnahmen können durch den **Verhältnismäßigkeitsgrundsatz** beschränkt werden (vgl. Art 24 DS-GVO).

# Sonstige EU-Rechtsgrundlagen?

---

- Die EU-Regelungen
  - **Data Governance-Act (DGA)**, (DGA, VO 2022/868):
  - **Digital Services Act (DSA)**
  - **EU-Data Act (DA)**, VO 2023/2854)
  - **AI Act** (VO 2024/1689)
  - **Single-Digital-Gateway** (SDG VO (EU) 2018/1724)
- enthalten wichtige Bestimmungen zur **Schaffung eines umfassenden Rechtsrahmenwerks für die Digitalisierung**
- aber **keine eigenen Rechtsgrundlagen** für die Datenverarbeitung im Sinne der DS-GVO.
- **Nationaler Gesetzgeber muss agieren!**

# Rechtsgrundlage: Einwilligung ?

- Nur erforderlich, wenn **keine andere Rechtsgrundlage** besteht,
- → ansonsten **Verarbeitung** u.U. **unverhältnismäßig!**
- **Art 4 Nr 11/Art 7 DSGVO** verlangen
  - **freiwillige**
  - **(aktive) Willensbekundung (!)**
  - in **informierter** Weise
  - auch über **jederzeitiges Widerrufsrecht!**
  - **Nachweismöglichkeit** des Verantwortlichen.

# Freiwilligkeit

---

- **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...“*
- **Konflikt mit Mitwirkungspflichten (§§ 60 ff SGB I)?**
- Problematisch auch im Bereich **Pflege** (Stichwort „**Demenz**“)
- Bei **Einsatz komplizierter Technologie** zudem fraglich, ob Betroffener versteht, was mit seinen Daten passiert!
- Auf **Datensicherheit** kann **nicht durch Einwilligung verzichtet** werden.

# Elektronische Gesundheitskarte/ Patientenakte

- **Nicht per Einwilligung, sondern per Gesetz!**
  - → **Gesundheitsdatennutzungsgesetz** (GDNG) vom 26.03.2024
  - → verpflichtend **Diagnosen, Medikamente als Pflichtangaben**
  - → Weitergabe zu **Forschungszwecken**
  - → **Verknüpfung** mit Daten der **klinischen Krebsregister** der Länder.
- Keine **echte Freiwilligkeit** durch **Einwilligung**,
- sondern **Verarbeitung auf gesetzlicher Grundlage** mit **Widerspruchsmöglichkeit** als **zusätzlicher Garantie**



# Datenschutzfragen bei KI-Systemen

---

- 1. Große **Datenmengen**
- 2. **Zweckändernde** Datenverarbeitung
- → zum **Training der Systeme**
- 3. Gefahr der Generierung **falscher Daten**,
  - Grundsatz der **Richtigkeit der Daten** (Art 5 DS-GVO)
  - **Large-Language-Modelle** erstellen Texte auf Grundlage reiner **Wahrscheinlichkeitsanalysen** (Probabilistik) → erhöhtes Risiko Erstellung „falscher Tatsachen“.

Automatisierte Verarbeitung mangels **voluntativen Elementes** keine Verarbeitung?

Verstößt gegen *Privacy by Design*.

# Lösung über Anonymisierung?

- Art. 4 Nr 1 DSGVO: **Personenbezogene Daten: alle Informationen**, die sich auf eine ....**identifizierbare natürliche Person**... beziehen; .... natürliche Person, die **direkt o. indirekt**, insbesondere mittels Zuordnung zu ...einem oder mehreren besonderen Merkmalen, **identifiziert werden kann**.
- **Keine Legal-Definition** der Anonymisierung (EG 27)
- -> Genügt noch „*unverhältnismäßiger Aufwand*“? (§ 67 Abs. 8 2. Alt. SGB X a.F.)
- → Problem der **schleichenden Reanonymisierung** durch **technischen Fortschritt**
- Die **Pseudonymisierung** (Art 4 Nr 5 DSGVO) **hebt Personenbezug nicht auf**, sondern kann Schwere des Eingriffs relativieren (h.M.).

# Künftig Pseudonymisierung = Anonymisierung?

---

- **EuGH vom 4.9.2025 - C-413/23, Celex-Nr. 62023CJ0413:**
- Eine Information bezieht sich auf eine identifizierte oder identifizierbare natürliche Person, wenn **aus Sicht der verarbeitenden Stelle eine Identifizierung möglich ist**; die **bloße Existenz zusätzlicher Zuordnungsinformationen führt nicht automatisch** dazu, dass pseudonymisierte Daten in jedem Fall und für jede Person als **personenbezogene Daten** zu qualifizieren sind.
- **Art 4 idF v Art 3 Digital Omnibus–E vom 15.11.2025:**
- „Angaben zu einer natürlichen Person sind **nicht notwendigerweise personenbezogene Daten** für jede andere Person oder Einrichtung, nur weil eine andere Einrichtung diese natürliche Person identifizieren kann; Angaben sind für eine bestimmte Einrichtung nicht personenbezogen, wenn diese Einrichtung die natürliche Person, auf die sich die Angaben beziehen, **in Anbetracht der mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel, nicht identifizieren kann**; derartige Angaben werden für diese Einrichtung nicht allein deshalb personenbezogen, weil ein **potenzieller späterer Empfänger über Mittel verfügt**, die mit hinreichender Wahrscheinlichkeit **zur Identifizierung** der natürlichen Person, auf die sich die Angaben beziehen, **verwendet werden können**;

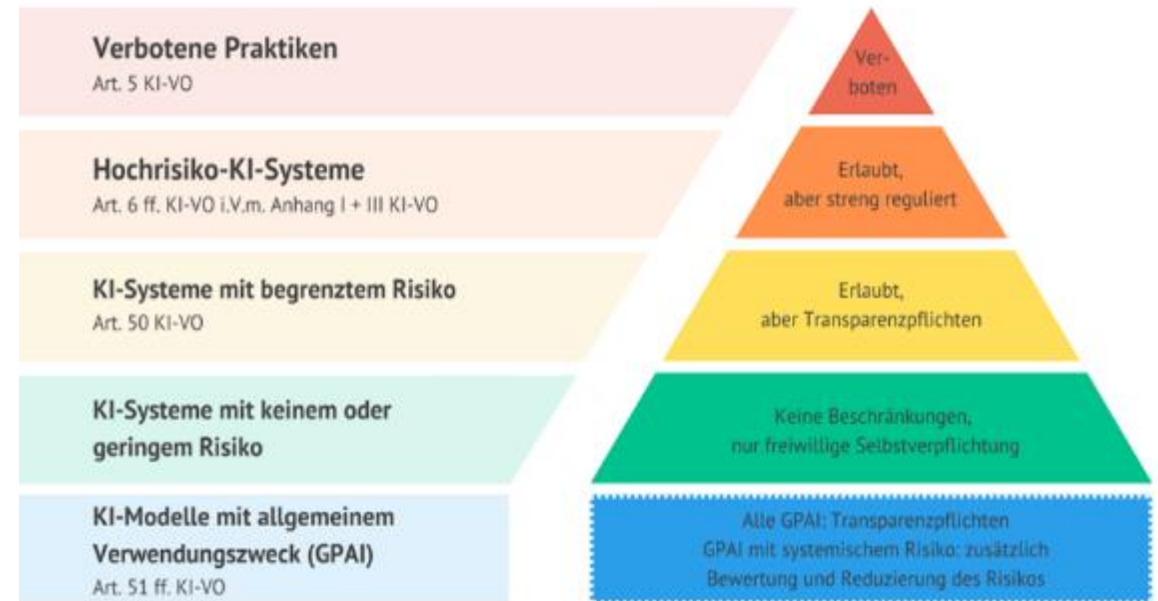
# Künftig Lockerung der Zweckbindung?

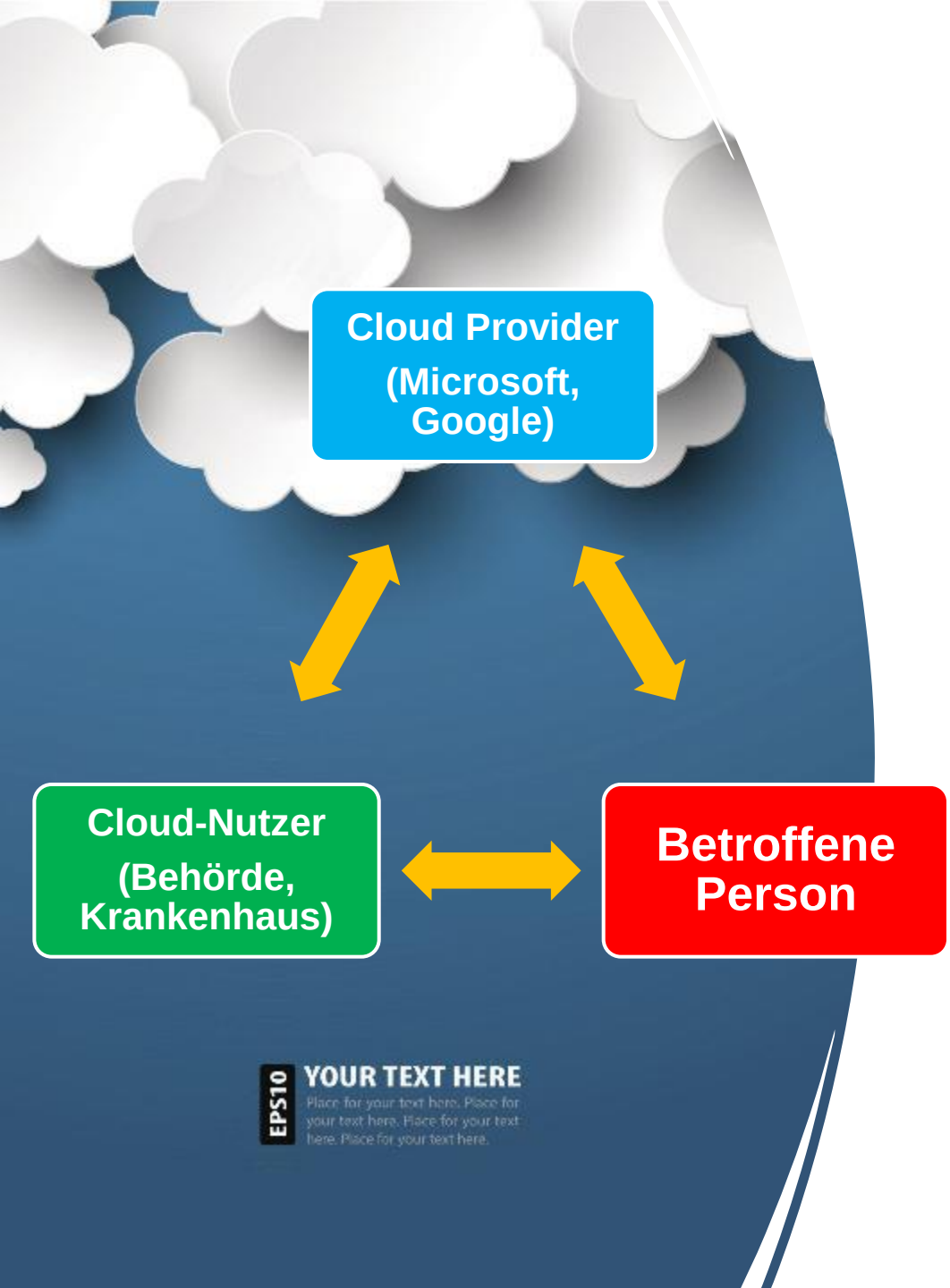
---

- Art 5 Abs 1 Buchst b DSGVO idF v Art 3 Digital Omnibus–E vom 15.11.2025
- Personenbezogene Daten müssen...
- *„für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; **eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Abs 1 als vereinbar mit den ursprünglichen Zwecken, unabhängig von den Bedingungen des Artikels 6 Absatz 4 dieser Verordnung („Zweckbindung“);...***
- Gilt das auch für **besondere Kategorien** von Daten (Art 9 DSGVO)?
- **Keine Einschränkung** durch **Mitgliedstaat** möglich (Art 9 Abs 4 DS-GVO)?
- Anlernung von KI = **wissenschaftlicher Zweck**?

# Einsatz von KI?

- **KI-VO (EU) 2024/1689** vom 13.6.2024 gibt nur bedingt Lösungen vor:
- → Definitionen
- → Risikoklassifizierungen
- **Art 22 Abs 3 DSGVO** erlaubt Einsatz von KI
- → Einwilligung
- → Gesetz
- → aber stets muss **individuelle Begründung** möglich sein!
- **Art 22 DSGVO idF v Art 3 Digital Omnibus–E** vom 15.11.2025 enthält nur Änderung der **Formulierung**, keine **inhaltliche Änderung**!





The diagram illustrates the cloud computing ecosystem. At the top, a blue box labeled 'Cloud Provider (Microsoft, Google)' is positioned within a stylized white cloud. Below it, a green box labeled 'Cloud-Nutzer (Behörde, Krankenhaus)' and a red box labeled 'Betroffene Person' are connected by a double-headed yellow arrow. Two additional double-headed yellow arrows connect the cloud provider box to each of the user and affected person boxes, indicating bidirectional communication. The background is a dark blue gradient with a white cloud graphic on the left.

Cloud Provider  
(Microsoft,  
Google)

Cloud-Nutzer  
(Behörde,  
Krankenhaus)

Betroffene  
Person

EPS10 YOUR TEXT HERE  
Place for your text here. Place for  
your text here. Place for your text  
here. Place for your text here.

# 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.
- Cloud Computing gilt als **Auftragsverarbeitung**
- -> Cloud-Provider ist **nicht Dritter** und es findet **keine Übermittlung** statt.
- → **§ 393 SGB V idF des DigiG** enthält wichtige Vorschriften zum Einsatz von Cloud-Diensten im Gesundheitswesen
- → C-5-Testat

# Auftragsverarbeitung in USA?

---

- Häufig befindet sich **Cloud Provider** im **Ausland**
- Auftragsverarbeitung darf **nur innerhalb der EU/EFTA** und **in Drittsaaten mit Angemessenheitsbeschluss** erfolgen (Art 49 DS-GVO, § 80 Abs 2 SGB X)
- USA wurden unter Voraussetzung von
  - **Safe Harbour**
  - **Privacy Shield** in *White-List* der Kommission aufgenommen.
- Der **EuGH** hat jeweils Beschlüsse der Kommission für unwirksam erklärt (EuGH vom 6.10.2015 – C 362/14 („**Schrems I**“)),
- zuletzt weil **Ombudsmechanismus** nicht mit Art 46 GRCh korrespondiert (*EuGH vom 16.7.2020 – C-311/18* („**Schrems II**“)).

# Übermittlung in USA

- Inzwischen im ***Trans-Atlantic Data Protection Framework*** wurde am 7.10.2022 durch US-Präsident Biden die „***Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities***“ erlassen:
- → Im Unterschied zum Ombudsverfahren nun Einführung eines **besonderen Gerichts** (*Data Protection Review (DP) Court*).
- Dort aber nur **klagebefugt** Bürger von Staaten, die kommerziellen Datenverkehr mit den USA zulassen
- **Angemessenheitsbeschluss der EU-Kommission** (Art 45 DS-GVO) **seit 10.7.2023**
- „**Schrems III**“? → **Nein** (EuG vom 3.9.2025 T-553/23)



# Digitale Souveränität Europas?

- **Europäische Alternativen zu Microsoft, Word** um Abhängigkeit von US-amerikanischen Softwareprodukten zu beenden, wegen....
- **Zugriffsrechte von US-Behörden auch in Europa?**
  - *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* statuiert **grundsätzliche Herausgabepflicht**
  - **United States District Court of Southern District of New York** vom 25.4.2014: => Verpflichtung von Microsoft in Europa gespeicherte Daten herauszugeben
- Außerdem Möglichkeit zum **Einfrieren von Daten!**
- **Sanktionen** wie im Fall Juge *Nicolas Guillou*.....
- Schleswig-Holstein wechselte bereits zu **alternativen Produkten**:
  - Office-Suite, LibreOffice Open-Xchange/Thunderbird (bereits in Nutzung).
  - Migration zu Linux 2026

# Fazit

- **Datenschutz ist Grundrechtsschutz und nicht nur Bürokratie**
- Relativierung des **Direkterhebungsgrundsatzes** im **Verhältnis zu Behörden** umsetzbar, bezüglich **Privaten** nur in Ausnahmefällen
- Datenschutz steht Digitalisierung nicht entgegen, sondern **flankiert Modernisierungsprozess**
- Datenschutz wirkt dabei stets **präventiv**; wenn Daten in unbefugte Hände geraten, ist der Schaden bereits eingetreten.
- Es gibt keine **absolute Datensicherheit**.
- Aber bestmöglicher Schutz vor Datenabfluss durch **technische Garantien** erforderlich.

# Digitale Zukunft

---

- Erforderlich ist intensiver Diskurs in der Gesellschaft, wie weit man Technik nutzen möchte trotz (immer) bestehender Restrisiken.