Karlsruher Institut für Technologie

Zentrum für Angewandte Rechtswissenschaft

Sensible pb. Daten, automatisierte Entscheidungen und KI

Dr. Christoph Werner

Vorlesung Datenschutzrecht
WS 2025/2026, UE 10/15

15.01.2026

wooclap.com Code: OINNUM

Agenda

1. Sensible pb. Daten nach Art. 9 DSGVO
2. Art. 22 DSGVO - Normtext
3. Art. 22 Abs. 1 – Erläuterung
4. Art. 22 Abs. 1 – Beispiele
5. Art. 22 Abs. 2 – Erlaubnistatbestände
6. Art. 22 Abs. 3 – besondere Betroffenenrechte
7. Art. 22 Abs. 4 – Verwendung sensibler Daten
8. Exkurs: KI-VO

1. Sensible pb. Daten nach Art. 9 DSGVO

1. Sensible pb. Daten nach Art. 9 DSGVO

Art. 9 Abs. 1: Die Verarbeitung personenbezogener Daten, aus denen die

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit hervorgehen, sowie […]
- genetischen Daten, (Art. 4 Nr. 13 DSGVO)
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art. 4 Nr. 14 DSGVO),
- Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

hervorgeht, ist untersagt. → Verbot mit Erlaubnisvorbehalt

1. Sensible pb. Daten nach Art. 9 DSGVO

Art. 9 Abs. 1: Beispiele und Grenzfälle
→ im Lichte des Diskriminierungsverbots (Art. 21 Abs. 1 GrC) auszulegen.

- rassische und ethnische Herkunft Beispielsweise Verarbeitung eines Fotos einer Person mit entsprechenden Merkmalen (z.B. Hautfarbe) dürfte nicht per se verboten sein, da nur äußerst beiläufige, unvermeidbare Erfassung (z.B. bei Foto auf Unternehmenswebseite)

  aber: **EuGH ZD 2023, 664 Rn. 69**: es kommt nicht darauf an, dass die Verarbeitung mit dem Ziel erfolgt, entsprechend sensible Informationen zu erhalten (Werbetracking z.B. auf Dating-Webseiten)

- genetischen Daten, (Art. 4 Nr. 13 DSGVO); genetisches Material selbst dürfte hierunter noch nicht fallen, sondern erst durch Digitalisierung

- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, (Art. 4 Nr. 14 DSGVO)

Vgl.: BeckOK DatenschutzR/Albers/Veit, 50. Ed. 1.8.2024, DS-GVO Art. 9 Rn. 34 f., 42 ff; weiterführend: Kohn/Schleper ZD 2023, 723

1. Sensible pb. Daten nach Art. 9 DSGVO

Art. 9 Abs. 1: Beispiele und Grenzfälle
→ im Lichte des Diskriminierungsverbots (Art. 21 Abs. 1 GrC) auszulegen.

- **Gesundheitsdaten**
  Art. 4 Nr. 15 DSGVO: „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

- Wie unmittelbar muss Gesundheitsbezug sein?
  - Hoher Alkohol-, Tabak- oder Fleischkonsum hinreichend? [1]
  - Pizzalieferung an psychiatrische Anstalt [2]
  - Foto mit Brille

[1] Vgl. Ablehnend: BeckOK DatenschutzR/Albers/Veit, 50. Ed. 1.8.2024, DS-GVO Art. 9 Rn. 34 f., 42 ff;
weiterführend: Kohn/Schleper ZD 2023, 723; [2] kritisch zu EuGH (vorangegangene Folie) mit diesem Beispiel: Golland, MMR 2023, 669 (681).

1. Sensible pb. Daten nach Art. 9 DSGVO

Omnibus-Verfahren (automatisierte Übersetzung):

Art. 9 Abs. 2 lit k) DSGVO-E Die Verarbeitung sensibler Daten ist zulässig, wenn die **„**Verarbeitung im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne von Artikel 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells unter den in Absatz 5 genannten Bedingungen.“ erfolgt

Art. 9 Abs. 5 DSGVO-E Für die Verarbeitung gemäß Absatz 2 Buchstabe k **werden geeignete organisatorische und technische Maßnahmen ergriffen, um die Erhebung und sonstige Verarbeitung besonderer Kategorien personenbezogener Daten zu vermeiden**. Erkennt der Verantwortliche trotz der Umsetzung solcher Maßnahmen in den für Lernen, Tests oder Validierungen verwendeten Datensätzen oder im KI-System oder KI-Modell **besondere Kategorien personenbezogener Daten, so entfernt er diese Daten**. Erfordert die Entfernung dieser Daten einen unverhältnismäßigen Aufwand, so **schützt der für die Verarbeitung Verantwortliche diese Daten** in jedem Fall wirksam und unverzüglich vor der Verwendung zur Erzeugung von Outputs, vor der Weitergabe oder anderweitigen Bereitstellung an Dritte.

Ausdehnung auch auf andere beiläufig erfasste, sensible pb. Daten?

1. Sensible pb. Daten nach Art. 9 DSGVO

Art. 9 Abs. 1: Beispiele und Grenzfälle
→ im Lichte des Diskriminierungsverbots (Art. 21 Abs. 1 GrC) auszulegen.

- **Gesundheitsdaten**
- **EuGH-Fall** (EuGH, v. 4.10.2024 – C-21/23, GRUR 2024, 1721, Rn. 76 ff.)
  - „alle personenbezogenen Daten, aus denen Informationen über den **früheren, gegenwärtigen und künftigen** körperlichen oder geistigen **Gesundheitszustand einer natürlichen Person hervorgehen**."
  - Ausreichend bereits, wenn aus den Daten „**mittels gedanklicher Kombination oder Ableitung** auf den Gesundheitszustand der betroffenen Person geschlossen werden kann" (Rn. 83 ff.)
  - Bestellung von **Arzneimittel** erlaubt solchen Rückschluss auf Gesundheitszustand; gilt auch soweit bestellende Person das Arzneimittel nicht zwangsläufig für sich kauft

1. Sensible pb. Daten nach Art. 9 DSGVO

- **Erlaubnistatbestände in Art. 9 Abs. 2 a-d**

a) Ausdrückliche Einwilligung

b) Auf Basis einer **Rechtsgrundlage** oder einer **Kollektivvereinbarung** im Arbeitsrecht, sowie im Recht der sozialen Sicherheit und des Sozialschutzes

c) Verarbeitung zum Schutz lebenswichtiger Interessen (+ fehlende Einwilligungsfähigkeit)

[1] Petri in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 9 Rn. 78

1. Sensible pb. Daten nach Art. 9 DSGVO

Vergleich Art. 6 lit d) zu Art. 9 Abs. 2 lit c) DSGVO

Art. 6 lit d)
die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

Art. 9 Abs 2 lit d) verlangt zusätzlich:
die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich **und**
die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben [keine Einwilligungsfähigkeit]

1. Sensible pb. Daten nach Art. 9 DSGVO

Umstritten, ob Vorrang der Einwilligung, d.h. subsidiäre Auslegung der lebenswichtigen Interessen auch bei Art. 6 lit d) bestehen sollte:

- **Contra (Einwilligungs(un)fähigkeit bei Art. 6 lit d) unbeachtlich)**
  - Wortlaut der Norm
  - Systematik: gestuftes Verhältnis von Art. 6, 9 [2]
    (sensiblere Daten → engerer Erlaubnistatbestand)

- **Pro (auch Art. 6 lit d) nur anwendbar, wenn keine Einwilligungsfähigkeit besteht)**
  - Telos: Selbstbestimmungsrecht gilt auch bzgl. DV bei lebenswichtigen Interessen [1]
  - EG 46, S. 2 DSGVO: Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann

Eher geringer Anwendungsbereich: nur bei Verarbeitung „normaler Daten“ (also z.B. Standortdaten, nicht Gesundheitsdaten) zu lebenswichtigen Zwecken und es wird trotz Einwilligungsfähigkeit keine Einwilligung erteilt (und es besteht auch keine sonstige RGL)

[1] Schulz in Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 49
[2] Kühling/Buchner, DS-GVO Art. 6 Rn. 110

1. Sensible pb. Daten nach Art. 9 DSGVO

- **Erlaubnistatbestände in Art. 9 Abs. 2 e-j DSGVO**

d) DV durch bestimmte Einrichtungen (Parteien, Gewerkschaften, Kirchen)

e) Daten offensichtlich selbst veröffentlicht (im Zusammenhang mit anderer RGL nach Art. 6)

f) Durchsetzung von Rechtsansprüchen

g) Rechtsgrundlage i.V.m. erheblichem öffentlichen Interesse
(qualifiziert ggü. Art. 6 Abs. 1 lit e)

h) Rechtsgrundlage zur individuellen Gesundheitsversorgung [1]

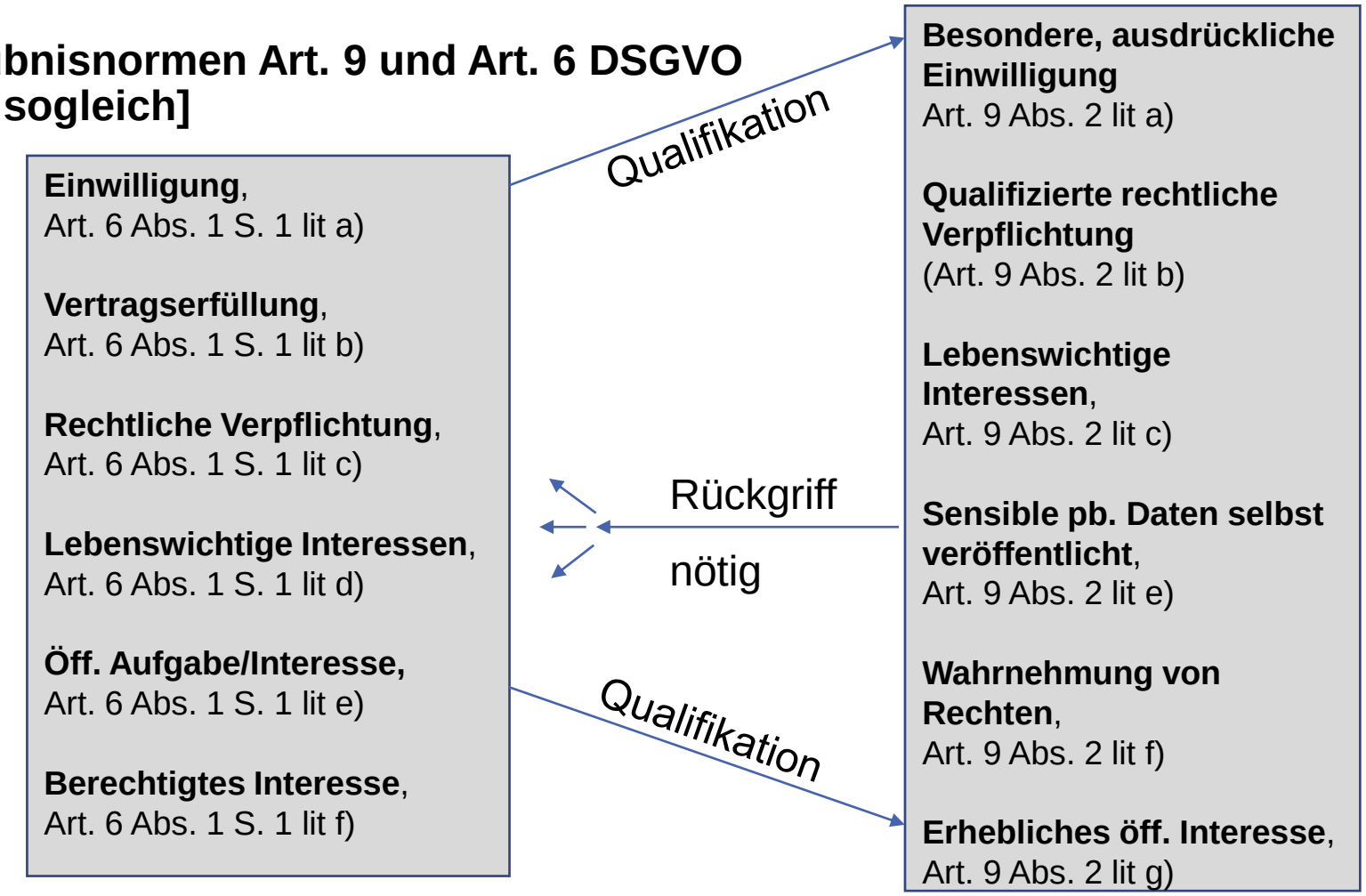
i) Rechtsgrundlage zur öffentlichen Gesundheit [1]

j) Rechtsgrundlage für archivarische, wissenschaftliche und statistische Zwecke (i.V.m. Art 89)

[1] Petri in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 9 Rn. 78

1. Sensible pb. Daten nach Art. 9 DSGVO

Verhältnis der Erlaubnisnormen Art. 9 und Art. 6 DSGVO [im Detail str., dazu sogleich]



1. Sensible pb. Daten nach Art. 9 DSGVO

Verhältnis der Erlaubnisnormen Art. 9 und Art. 6 DSGVO

- **Ist umstritten** [1] **: wenig hilfreich auch EG 51, S. 5:** Zusätzlich zu den speziellen Anforderungen [nach Art. 9] an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten.

  m.E. **keine pauschale Lösung**

  - Zumeist Qualifikation: Besonders verschärfte RM-Tatbestände, z.B. bei Einwilligung [2], Lebenswichtige Interessen (+ Erfordernis der Einwilligungsunfähigkeit, str.); erhebliches öffentliches Interesse

  - „Rückgriff“: bei selbst öffentlich gemachten Daten (Art. 9 Abs. 2 lit e) DSGVO
    → dann aber Rückgriff auf Tatbestände nach Art. 6 DSGVO, insb. Art. 6 Abs. 1 lit f)

- **Zweckänderungen (Art. 6 Abs. 4)** auch im Rahmen des Art. 9 möglich
  Arg.: Sensible Daten im Wortlaut genannt: **Art. 6 Abs. 4 lit c**; gesteigerte Anforderungen

[1] Matjek/Mäusezahl, ZD 2019, 551 (554)
[2] Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 23; Kampert in Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, DS GVO Art. 9 Rn. 62

Art. 22 DSGVO – Verbot automatisierter Entscheidungen

2. Art. 22 DSGVO: Normtext

Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, **nicht** einer **ausschließlich auf einer automatisierten Verarbeitung** – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, [...] zulässig ist und diese Rechtsvorschriften **angemessene Maßnahmen** zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

2. Art. 22 DSGVO: Normtext

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen**, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren,** wozu mindestens

- das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen,
- auf Darlegung des eigenen Standpunkts und
- auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen **nicht** auf **besonderen Kategorien personenbezogener Daten** nach Artikel 9 Absatz 1 beruhen, **sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g** gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Art. 9 Abs. 1 lit a):	ausdrückliche Einwilligung [in die Verarbeitung besonderer Kategorien personenbezogener Daten]
Art. 9 Abs. 1 lit g):	Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats aus Gründen eines erheblichen öffentlichen Interesses

Art. 22 Abs. 1 DSGVO: Erläuterung

- Entscheidung „Eine Entscheidung ist die Festlegung auf ein bestimmtes Ergebnis. Es muss daher ein gestaltender Akt mit abschließender Wirkung vorliegen.“

- Die Entscheidung muss eigenständig gestaltend sein, d.h. insb. **keine bloße Bestätigung** einer bereits vertraglich festgelegten Entscheidung, insbesondere bei vertraglich festgelegte Wenn-Dann-Entscheidungen, z.B. Parkplatz-Schranke

- Der Betroffene muss der Entscheidung „unterworfen“ sein, was ein **einseitiges Festlegen der Bedingungen** der Verarbeitung und der Grundlagen der Entscheidungsfindung durch den Verantwortlichen voraussetzt (nicht z.B. bei frei konfigurierbarem Smarthome)

- Ausschließlich beruhend auf einer automatisierten Verarbeitung einschließlich Profiling

  Umkehrschluss: Zulässigkeit (+), wenn Mensch als aktiv prüfende Kontrollinstanz oder automatisierte Entscheidung als Hilfsmittel bzw. Teilverarbeitung zulässig, soweit bestimmendes Element bei einem Menschen verbleibt
- (-) wenn nur formal ein Mensch zwischengeschaltet wird (z.B. muss bloß Häkchen setzen oder hat gar keine Qualifikation)

BeckOK IT-Recht, Borges/Hilber/*Steinrötter,* Rn. 5-9.

3. Art. 22 Abs. 1 DSGVO: Erläuterung

„Profiling“, Art. 4 Nr. 4 DSGVO das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter **Bewertung der persönlichen Aspekte** in Bezug auf eine natürliche Person besteht, **insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel** der betroffenen Person

Wichtigste Anwendungen:

- Empfehlungssysteme (Recommender Systems)
  - Für Sozial Media und Suchmaschinen (Filter Bubble)
  - Für Produkte (Amazon, Netflix)
- Marketing (webseitenübergreifendes Tracking: Cookies; Payback-Karten und sonstige Einkaufs-Apps)
- Kreditscoring

Problematik: äußerst aussagekräftige Persönlichkeitsprofile ermöglichen
a) mehr oder minder persönlichkeitsrelevante „Manipulation“;
b) können ggf. für andere Zwecke weitergegeben werden

3. Art. 22 Abs. 1 DSGVO: Erläuterung

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

- **„rechtliche Wirkung entfaltet“** jegliche Rechtswirkung, strittig, ob auch *positive* Wirkung – aber eher ja, weil es nicht auf die Wirkung im Einzelfall ankommen kann sondern ein „Vorfeldschutz“ nötig ist [1]

- **„in ähnlicher Weise erheblich beeinträchtigt“** Wirkungen durch tatsächliches Handeln oder Realakte; erheblich: persönliche oder finanzielle Interessen der betroffenen Person werden mit einem gewissen Umfang und/oder mit einer gewissen Dauer negativ tangiert
  z.B.: Ablehnung bei Verträgen die erhebliche Auswirkung auf das Leben einer Person haben (Arbeitsplatzbewerbungen, Kredite, Gesundheitsdienstleistungen) [2]

[1] Paal/Pauly/*Martini,* Art. 22 DSGVO Rn. 28.]
[2] Art.-29-Gruppe, WP 251 rev.01, S. 23

4. Art. 22 Abs. 1 DSGVO - Beispiele

Beispiel 1: Direktwerbung an eine Person, die auf deren Nutzerverhalten eines Systems angepasst ist

- Automatisierte Entscheidung? *Ja, die Auswahl der Werbung wird nicht durch eine Person getroffen*
- Erhebliche Betroffenheit?
  - Rechtswirkung *keinerlei rechtliche Wirkung*
  - Ähnliche Beeinträchtigung *keine anderweitige Einwirkung – keine Beeinträchtigung der Interessen*

Ergebnis: wohl nein - (Exkurs: ebenso wenig Suchmaschinenergebnisse, da ebenfalls keine hinreichend erhebliche Wirkung) [str., siehe [1]]; Gegenargument: erhebliche Beeinträchtigung des Persönlichkeitsrechts durch personalisierte Werbebeinflussung oder bei Suchmaschinenergebnissen der Informationsfreiheit

Aber Art 26 Abs. 3 DSA: „Die Anbieter von Online-Plattformen **dürfen Nutzern keine Werbung anzeigen**, die auf Profiling gemäß Artikel 4 Nummer 4 [Legaldefinition] der Verordnung (EU) 2016/679 **unter Verwendung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1** der Verordnung (EU) 2016/679 beruht.

[1] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 22, Rn. 40, Fn. 155 m.w.N.

Exkurs: Der Digital Services Act (DSA)

Zielt auf mehr Sicherheit, Transparenz und Verbraucherschutz im Internet

Adressiert insb. sehr große digitale Plattformen und Dienste (z.B. Google, Meta (Instagram, Facebook), Amazon)

Verlangt in Art. 34 Abs. 1 ein Risikomanagement mit Blick auf systemische Risiken wie

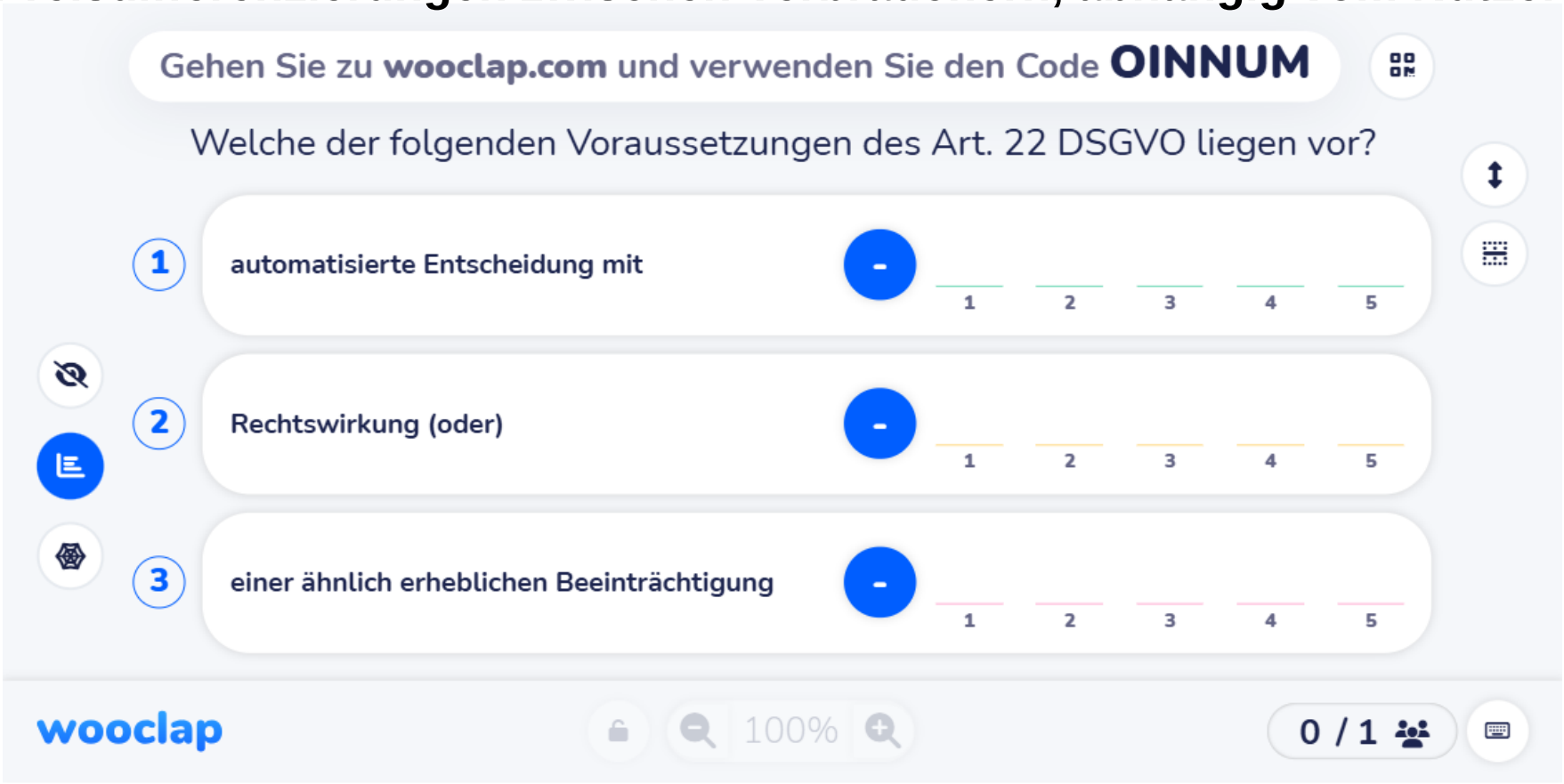
- **Verbreitung rechtswidriger Inhalte (Hetze, Beleidigungen)** über ihre Dienste
- nachteilige **Auswirkungen auf die Ausübung der Grundrechte** wie Achtung der Menschenwürde, Achtung des Privat- und Familienlebens, Schutz personenbezogener Daten, die Meinungs- und Informationsfreiheit
- alle tatsächlichen oder absehbaren nachteiligen Auswirkungen auf die **gesellschaftliche Debatte** und **auf Wahlprozesse** und die öffentliche Sicherheit

- Nach Art. 34 Abs. 2 sind hierbei insbesondere die [angepasste]
  - Gestaltung ihrer Empfehlungssysteme und anderer relevanter algorithmischer Systeme sowie Systeme zur Moderation von Inhalten

D.h. **abstrakte Anforderungen an AE** (welche Inhalte werden angezeigt/gefiltert), unabhängig von Entscheidung (mit rechtlicher oder vergleichbarer Wirkung) i.S.d. Art. 22 DSGVO an eine betroffene Person.

4. Art. 22 Abs. 1 DSGVO - Beispiele

Beispiel 2: Preisdifferenzierungen zwischen Verbrauchern, abhängig vom Nutzerverhalten



4. Art. 22 Abs. 1 DSGVO - Beispiele

Beispiel 2: Preisdifferenzierungen zwischen Verbrauchern, abhängig vom Nutzerverhalten

- Automatisierte Entscheidung? *Ja, denn sie wird autonom durch das System getroffen*
- Erhebliche Betroffenheit?
  - Rechtswirkung *Nein, denn es liegt nur ein Angebot und keine Bindung vor*
  - Ähnliche Beeinträchtigung *Nein, solange keine Störung der wirtschaftlichen Entfaltung oder Diskriminierung vorliegt -> Abweichung in der Praxis meist gering*

Ergebnis: Anwendungsbereich jedenfalls bei geringfügigen Preisdifferenzen nicht eröffnet [1]

Art. 246a, § 1 Abs. 1 Nr. 6 EGBGB: Pflicht zum Hinweis, „dass der Preis auf der Grundlage einer automatisierten Entscheidungsfindung personalisiert wurde,“

[1] Martini in Paal/Pauly, Art. 22, 4. Aufl. 2021, Rn. 27a f.

4. Art. 22 Abs. 1 DSGVO - Beispiele

Beispiel 3: Kredit-Scoring-Verfahren:

- automatische Ablehnung eines Online-Kreditantrags
  (+) da hier tatsächliche Entscheidung des „Ob“ eines Kredites durch das System getroffen wird

- Score-Wert der externen Auskunftei (Schufa) erfasst?
  - **Contra:** noch keine unmittelbare Wirkung; Entscheidung etwa über Kredite, Mietvertrag etc. wird nicht von der Schufa getroffen; somit eher vorbereitende AV

  - **Pro:** Beeinträchtigung bereits durch Score-Entscheidung; Andernfalls droht außerdem möglicherweise Regelungslücke bei Auskunfts- und anderen Betroffenenrechten;

[Blasek, ZD 2022, 433]

4. Art. 22 Abs. 1 DSGVO - Beispiele

Beispiel 3: Kredit-Scoring-Verfahren:

Entscheidung EuGH v. 07.12.2023, Az. C-634/21, NZA 2024, 45:

► Schließt sich der Pro-Seite an, d.h.:

- Ermittlung des Score-Werts ist bereits eine Entscheidung i.S.v. Art. 22 Abs. 1 DSGVO;
- Hat auch rechtliche Wirkung, soweit Dritte (z.B. Banken) von diesem Wert „maßgeblich“ geleitet werden (was laut Vorlagegericht bei Banken fast immer der Fall ist)
- Andere Auslegung birgt Gefahr einer Umgehung/Rechtsschutzlücke

[Blasek, ZD 2022, 433]

4. Art. 22 Abs. 1 DSGVO - Beispiele

Weitere Beispiele für automatisierte Entscheidungen:

- Auswahl von Organspendeempfänger:innen (sensible Daten)
- Auswahl von Bewerbern oder Arbeitnehmern
  - **E-Recruiting:** Der Bewerber gibt seine Daten ein und erhält eine Absage des Systems, weil er eine bestimmte Punktzahl nicht erreicht hat
  - **Bewerberranking** zur Entscheidungsunterstützung ist aber möglich, solange die Auswahl noch keine endgültige Entscheidung trifft [1];
  - ggf. nun Auslegung des EuGH beachten: „Maßgeblichkeit“

[Blasek, ZD 2022, 433]

5. Art. 22 Abs. 2 - Erlaubnistatbestände

Zulässigkeit AE nach Abs. 2: *Wann darf ich das?*
(betrifft nur die automatisierte Entscheidung, nicht die Verarbeitung als solches)

Art. 22 Abs. 2 lit

a) Für **Vertragsschluss oder -erfüllung erforderlich**
z.B. Geschäfte, bei denen die Entscheidung durch ein automatisiertes System notwendig ist, weil sonst das Produkt nicht funktioniert (z.B. automatisierte Fahrzeuge)

b) durch **angemessene gesetzliche Legitimation** zulässig,
z.B. § 37 BDSG - Leistungserbringung aus Versicherungsvertrag

c) mit **ausdrücklicher Einwilligung der** betroffenen Person

6. Art. 22 Abs. 3 – besondere Betroffenenrechte

- Recht auf **Erwirkung des Eingreifens einer Person** seitens des Verantwortlichen
  es muss in begründeten Härtefällen (nicht vorbehaltlos) [1] die Möglichkeit geben, sich an den Verantwortlichen zu wenden und eine Entscheidung einer natürlichen Person herbeizuführen

- **Darlegung des eigenen Standpunktes** der betroffenen Person
  zB durch Freitextfelder in Online-Formularen

- **Anfechtung** der (automatisierten) Entscheidung
  Recht auf erneute Kontrolle der automatisierten Entscheidung

- **Art. 13 Abs. 2 lit f, Art. 15 Abs. 1 lit h DSGVO**
  Zu informieren, Auskunft zu erteilen über: „das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – **aussagekräftige Informationen über die involvierte Logik** sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.“
  [Grenze des Geschäftsgeheimnisschutzes, außerdem schwierig bei KI]

[1] Martini in Paal/Pauly 3. Aufl. 2021, DS-GVO Art. 22 Rn. 39a

6. Art. 22 Abs. 3 – besondere Betroffenenrechte

Praxisfall: Betroffene Person P konnte seinen Mobilfunkvertrag nicht verängern, der Mobilfunkanbieter lehnte dies aufgrund schlechter Bonität ab. Diese wurde von der Auskunftei D&B bewertet. P wandte sich daraufhin an die Aufsichtsbehörde A, diese wies die D&B an, „aussagekräftige Informationen über die involvierte Logik der auf der Grundlage der personenbezogenen Daten von CK erfolgten automatisierten Entscheidungsfindung zu übermitteln.“ und so ihre Auskunftspflicht nach Art. 15 Abs. 1 lit h DSGVO zu erfüllen.

Wie muss sich die D&B verhalten?

6. Art. 22 Abs. 3 – besondere Betroffenenrechte

6. Art. 22 Abs. 3 – besondere Betroffenenrechte

Lösung:

- **Detaillierte, verständliche Erklärung (Antwortmöglichkeit 3) erforderlich**

- Auskunftsrecht soll insbesondere auch ermöglichen Reche wie die Anfechtung der Entscheidung und die Darlegung des eigenen (abweichenden) Standpunkts zu ermöglichen; setzt volles Verständnis der automatisierten Entscheidungsfunktion voraus [Rn. 55f.]

- Übermittlung des Algorithmus oder einer detaillierten Beschreibung der [technischen] Schritte für sich genommen hinreichend [Rn. 59], da nicht ausreichend präzise und **verständlich**

- Vielmehr muss die AE so **konkret beschrieben** werden, „dass die betroffene Person nachvollziehen kann, welche ihrer personenbezogenen Daten iRd in Rede stehenden automatisierten Entscheidungsfindung auf welche Art verwendet wurden.“ [Rn. 61]. „Das vorlegende Gericht [könnte] es insb. als ausreichend transparent und nachvollziehbar erachten, die betroffene Person zu informieren, in welchem Maße eine Abweichung bei den berücksichtigten personenbezogenen Daten zu einem anderen Ergebnis geführt hätte.“ [Rn. 62]

7. Art. 22 Abs. 4 – Verwendung sensibler Daten

bei Verarbeitung sensibler personenbezogener Daten: Art. 22 Abs. 4 DSGVO
die Entscheidung aus der Verarbeitung von Daten bzgl. der Kategorien des Art. 9 Abs. 1 DSGVO ist grundsätzlich unzulässig

Ausnahme:

- automatisierte Verarbeitung nach Art. 22 Abs. 2 wird durch Verarbeitungsgrundlage des **Art. 9 Abs. 2 lit. a** (ausdrückliche Einwilligung) oder **lit. g** (gesetzliche/unionsrechtliche Legitimation, § 22 Abs. 1 BDSG) ergänzt **und**

- angemessene **TOM**s wirken erhöhtem Risiko entgegen, d.h. ggf. weiteres Hinzutreten von Maßnahmen, „ausführlicher“ in § 22 Abs. 2 BDSG

8. Exkurs KI-VO (VO 2024/1689)

8. Exkurs KI-VO

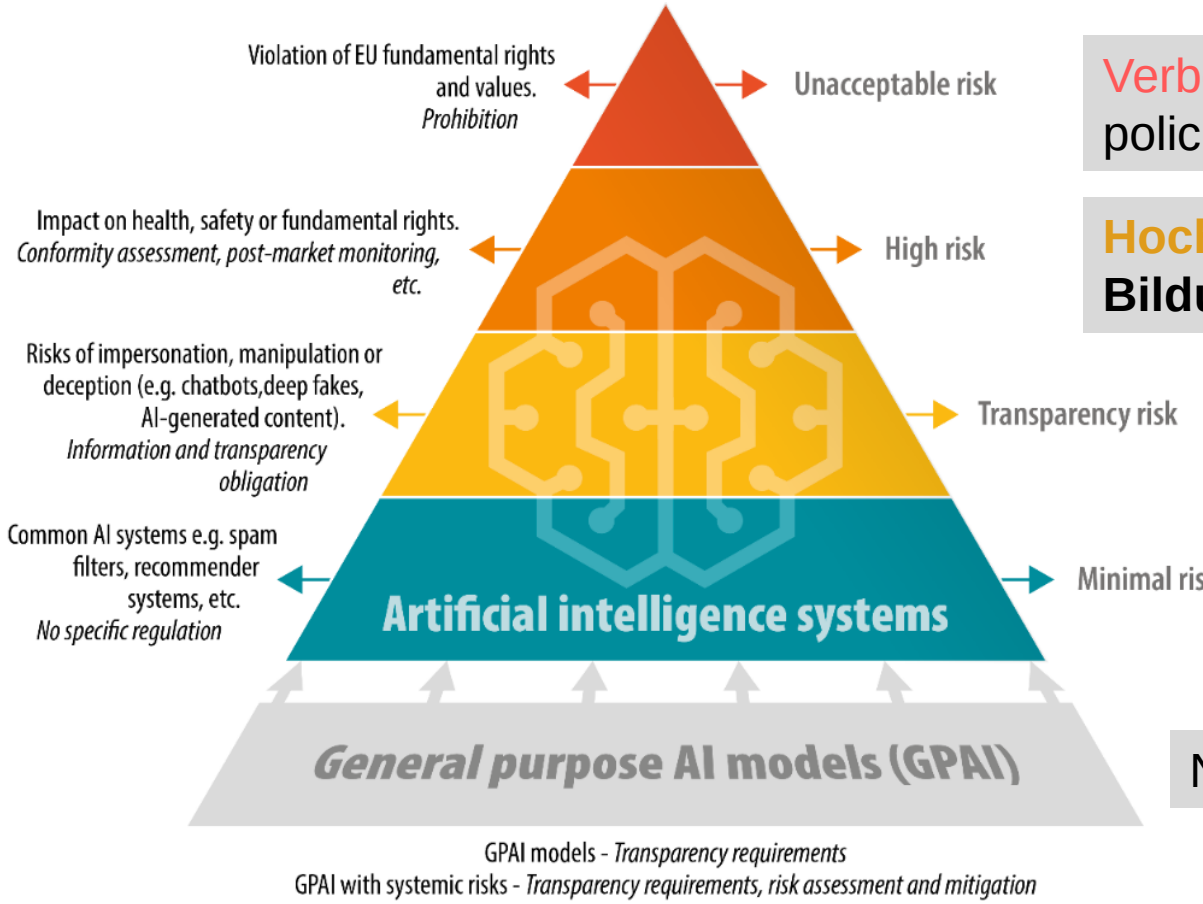
Adressiert KI-Systeme, die in Art. 2 Nr. 1 KI-VO definiert werden als „ein **maschinengestütztes System**, das

- für einen in **unterschiedlichem Grade autonomen Betrieb** ausgelegt ist und
- das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und
- das aus den **erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden**, die physische oder virtuelle Umgebungen beeinflussen können.“

(Aufzählungszeichen aus Gründen der Lesbarkeit ergänzt)

8. Exkurs KI-VO

Sektorübergreifende Regelung, d.h. grds. alle KI-Systeme, unabhängig von Einsatzzweck und Branche, aber mit **risikobasiertem Ansatz**:



Verbotene KI-Anwendungen, z.B. Social scoring, predictive policing, grds. Emotionserkennung in Bildung und Arbeit

Hoch-Risiko: **z.B. Personalrecruting, Medizinprodukte, Bildung (u.a. Zulassung, Bewertung)**

Begrenztes Risiko: z.B. Chatbots;
v.a. Informationspflichten (Transparenz, Art. 50 KI-VO)

Minimales oder kein Risiko: keine Einschränkungen

Nachträglich ergänzt: GPAI (mit systemischem Risiko)

Quelle Abbildung: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf, S.8

8. Exkurs KI-VO

Hoch-Risiko-KI-Systeme, u.a. Systeme die in den Bereichen Medizin, Kredit-Scoring, Bildung, Beschäftigung, Strafverfolgung, Migration und Rechtspflege eingesetzt werden (i.d.R. auch mit personenbezogene Daten)

Verhältnis der KI-VO zur DSGVO

- Diese Verordnung berührt nicht die […] [DSGVO], unbeschadet des Artikels 10 Absatz 5 und des Artikels 59 der vorliegenden Verordnung.

- **D.h. grundsätzlich findet die DSGVO uneingeschränkt Anwendung**, d.h. für die **Verarbeitung** der Daten (Trainingsdaten, Eingabedaten, Ausgabedaten) gilt die DSGVO, soweit es sich um **personenbezogene Daten** handelt.

Nutzer:in: *Ich benötige Hilfe für meine Datenschutzklausur, die Aufgabe ist…*

ChatGPT: *Gerne…*

Quelle: Vortragsfolien mit Fotos von Jonas Siglmüller, DGRI 2023

8. Exkurs KI-VO

Sonderregelungen:

- Art. 10 Abs. 5 KI-VO: erlaubt u.U. auch die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO), soweit dies zur Erkennung und Korrektur von Verzerrungen unbedingt erforderlich ist.

- Art. 59 KI-VO: Zweckändernde (Art. 6 Abs. 4 DSGVO) Nutzung personenbezogener Daten in behördlichen KI-Reallaboren (Art. 3 Nr. 55 KI-VO), wenn KI-Systemen erheblichem öffentlichem Interesse dienen (z.B. öffentliche Gesundheit, Umweltschutz, nachhaltige Energieversorgung)

- Omnibus-Verfahren: Art. 9 Abs. 2 lit k), Abs. 5 DSGVO-E
  Zulässigkeit der Verarbeitung sensibler Daten für Entwicklung und Betrieb eines KI-Systems + Regelung für beiläufig erfasste sensible Daten (siehe im Detail Folie

8. Exkurs KI-VO

Überschneidung mit Art. 22 DSGVO, da i.d.R. rechtliche oder ähnlich erhebliche Wirkung, d.h. KI-Einsatz nur erlaubt wenn

- Erlaubnistatbestand nach Art. 22 Abs. 2 DSGVO vorliegt und
- wenn Entscheidung tatsächlich durch KI getroffen wird („ausschließlich beruhend“), nicht bloß unterstützend

Beispiel: KI gestütztes E-Recruiting mit negativer Vor-Filterung (d.h. Bewerber:innen werden von der KI abschließend aussortiert)

- Arbeitsvertragsablehnung = ähnliche erhebliche Beeinträchtigung i.S.d. Art. 22 Abs. 1 (+)
- Art. 22 Abs. 2 lit c) Einwilligung? **P: Freiwilligkeit,** lit a) für Vertragsschluss **erforderlich (P)**
- Hoch-Risiko-System nach KI-VO, d.h. Informationspflichten (Art. 50) sowie Informationspflichten nach DSGVO (Art. 12 ff. DSGVO)
- Anforderungen an Safety und Security nach KI-VO und DSGVO, dazu nächste Folie

8. Exkurs KI-VO

Anforderungen an Security und Safety

Art. 15 Abs. 1 KI-VO: „Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie im Hinblick auf ihre Zweckbestimmung ein **angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen** und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.“

EG 71 S. 6 DSGVO: Um […] eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, **die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird**, und personenbezogene Daten in einer Weise **sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen** wird [..] (Safety)

Art. 32 DSGVO: risikoangemessenes Datensicherheitsniveau (Security)

Mehr zur „Data Security“ in der DSGVO in UE 11/15

8. Exkurs KI-VO

Anforderungen an Verfahren

Art. 35 DSGVO: Datenschutzfolgenabschätzung verlangt ein umfassendes Risikomanagement mit Risikobeschreibung, Bewertung und Bewältigung durch entspr. Abhilfemaßnahmen (z.B. hinsichtlich Datensicherheit, durch Pseudonymisierung, besonderes Controlling, usw.), soweit *voraussichtlich hohes Risiko für Rechte und Freiheiten natürlicher Personen besteht*

Aber nach Art. 35 Abs. 3 immer bei risikoreichen Verarbeitungstätigkeiten, dazu gehört u.a.:

1. **Anwendungsfällen des Art. 22 DSGVO, sofern Profiling mit Entscheidung vorliegt**
2. Umfassender Verarbeitung sensibler Daten **(Art. 22 Abs. 4)**
3. EG 91, S. 1 „in großem Umfang eine neue Technologie eingesetzt wird“)

8. Exkurs KI-VO

Anforderungen an Verfahren

Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme (Art. 27 KI-VO)

- **„die spezifischen [grundrechtlichen] Schadensrisiken**, die sich auf die gemäß Buchstabe c dieses Absatzes ermittelten Kategorien natürlicher Personen oder Personengruppen auswirken könnten.“

- **Aber** Art. 27 Abs. 4 KI-VO: Wird eine der in diesem Artikel festgelegten Pflichten bereits infolge einer gemäß Artikel 35 der Verordnung (EU) 2016/679 […] durchgeführten Datenschutz-Folgenabschätzung erfüllt, so **ergänzt** die Grundrechte-Folgenabschätzung gemäß Absatz 1 des vorliegenden Artikels diese Datenschutz-Folgenabschätzung.

8. Exkurs KI-VO

Ergebnis:

- Hoher Überschneidungsbereich zwischen DSGVO und KI-VO
  1. Durch Verarbeitung personenbezogener Daten
  2. Insbesondere durch Vorliegen automatisierter Entscheidungen nach Art. 22 DSGVO v.a. bei Hoch-Risiko-KI-Systemen

- Überlappende Vorgaben an Security, Safety sowie beim Risikomanagement-Verfahren

- Gemeinsame Betrachtung der rechtlichen Vorgaben geboten.

Gesamtübersicht Erlaubnistatbestände

Verbot mit Erlaubnisvorbehalt

+ ggf. Beachtung der KI-VO

Verarbeitung „normaler“ pb. Daten

Art. 6 Abs. 1 lit a-f)

z.B. Einwilligung, Erfüllung eines Vertrages, Rechtspflicht, öff. Interesse berechtigtes Interesse

Verarbeitung „sensibler“ pb. Daten

Art. 9 Abs. 2 lit a-j)

z.B. explizite Einwilligung, spezifische Rechtspflicht, erhebliches öff. Interesse

Automatisierte Entscheidung

Art. 22 Abs. 2 lit a-c)

Explizite Einwilligung, Rechts-vorschrift, Erfüllung eines Vertrags

Meist qualifiziert, alternativ

Additiv (beachte auch Art. 22 Abs. 4)