Karlsruher Institut für Technologie

Zentrum für Angewandte Rechtswissenschaft

# Datensicherheit und IT-Sicherheit

**Dr. Christoph Werner**


Vorlesung Datenschutzrecht
WS 2025/2026, UE 11/15

22.01.2026

Wooclap.com Code: BLEJLO

# Agenda

0. Nachtrag: Exkurs KI-VO

1. Übersicht über Art. 24, 25, 32 DSGVO

2. Art. 24 – Verantwortung des für die Verarbeitung Verantwortlichen

3. Art. 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Data protection by Design and by default)

4. Art. 32 – Sicherheit der Verarbeitung (Security of processing)

5. Datensicherheit und IT-Sicherheit

# 0. Nachtrag: 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

# 0. Nachtrag: 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“)

# 0. Nachtrag: 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.

# 0. Nachtrag: 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“ Daten**

Art. 6 Abs. 1 lit a-f)

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

**Verarbeitung „sensibler“ 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)

# 1. Übersicht über Art. 24, 25, 32 DSGVO

**Gemeinsamkeiten:** all diese Vorschriften verlangen vom Verantwortlichen bzw. dem Auftragsverarbeiter **risikoangemessene, technische und organisatorische Maßnahmen** zu ergreifen.

D.h. kein formelles Datenschutzrecht mehr, sondern praktische Handlungspflichten

- **technischen Maßnahmen** zählt man eher solche, die sich auf den (elektronischen) Datenverarbeitungsvorgang selbst erstrecken (Software zur Datenverwaltung, Datensicherheitsfunktionen, elektronische Kontaktmöglichkeiten)
- **Organisatorische Maßnahmen** beziehen sich auf den äußeren Ablauf bei der Datenverarbeitung (Schulungen der Mitarbeiter, Vieraugenprinzip)“
- **Abstrakte Eignung vorausgesetzt; keine isolierende Unterteilung zwischen technisch und organisatorisch**

[BeckOK DatenschutzR/Schmidt/Brink, 42. Ed. 1.5.2022, DS-GVO Art. 24 Rn. 15]

# 1. Übersicht über Art. 24, 25, 32 DSGVO

| | Art. 24 Abs. 1 DSGVO | Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f DSGVO | Art. 32 Abs. 1, 2 DSGVO |
|---|---|---|---|
| **Einheitliche, zu berücksichtigende Kriterien** | Modalitäten der Verarbeitung (Art, Umfang, Umstände, Zwecke)<br>Risiko für Rechte und Freiheiten natürlicher Personen (risikobasierter Ansatz) | | |
| **Besondere, zu berücksichtigende Kriterien** | | Stand der Technik<br>Implementierungskosten | Stand der Technik<br>Implementierungskosten |
| **Schutzzweck** | nachweisbare Einhaltung der DSGVO | Wirksame Umsetzung der Datenschutzgrundsätze + entsprechender Garantien | Gewährleistung eines risikoangemessenen Schutzniveaus |
| **Handlungsauftrag** | Geeignete technische und organisatorische Maßnahmen | | |
| **Adressat** | Verantwortlicher | Verantwortlicher | Verantwortlicher + Auftragsverarbeiter |
| **Gewährleistung von Vertraulichkeit und Integrität bzw. Verfügbarkeit** | | i.V.m. Art. 5 lit f):<br>**in einer Weise verarbeitet werden**,<br>die insb. Schutz gewährt vor:<br><br>unbefugter oder unrechtmäßiger **Verarbeitung**;<br>**[Innenschutz]**<br><br>unbeabsichtigtem/er Verlust, Zerstörung, Schädigung | Minimierung von Risiken durch<br><br>**unbefugte Offenlegung unbefugten Zugang [Außenschutz]**<br><br>unbeabsichtigte oder unrechtmäßige(r) Vernichtung, Verlust oder Veränderung<br><br>von Daten, die<br>„**verarbeitet wurden“** |

# 2. Art. 24 DSGVO

**Art 24 Abs. 1:** Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um **sicherzustellen** und den **Nachweis** dafür erbringen zu können, dass die **Verarbeitung gemäß dieser Verordnung** erfolgt. [2]Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

- **Grundnorm; zentrale Regelung für die umfassende Verantwortung des „Verantwortlichen“**
- Pflicht zur Vornahme **technische und organisatorische Maßnahmen**
- **Zur Einhaltung der Verordnung**
  - Datenschutzmanagement, Hard- und Software zur Datenverwaltung, elektronischer Umgang mit Betroffeneneingaben, Sensibilisierung der Mitarbeiter für Datenschutz
- **Und den entsprechenden Nachweis** (z.B. it-gestützte Verfahrensverzeichnisse, Art. 30 DSGVO )

# 3. Art. 25 Abs. 1 DSGVO

**(1) – Datenschutz durch Technikgestaltung („privacy by design“)**

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der [Modalitäten] der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft **der Verantwortliche** sowohl **zum Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch **zum Zeitpunkt der eigentlichen Verarbeitung** geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung, die dafür ausgelegt sind, **die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen** und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

# 3. Art. 25 Abs. 1 DSGVO

**(1) – Datenschutz durch Technikgestaltung („privacy by design“)**

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der [Modalitäten] der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft **der Verantwortliche** sowohl **zum Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch **zum Zeitpunkt der eigentlichen Verarbeitung** geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung, die dafür ausgelegt sind, **die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen** und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

**Adressaten:**

- Nur **Verantwortlicher** iSd Art. 4 Nr. 7 DSG-VO (nicht der Auftragsverarbeiter!)
- Die **Hersteller** von Produkten, Diensten und Anwendungen sind demgegenüber nicht dem Pflichtenkatalog unterworfen [EG 78]
- Der Mechanismus „privacy by design“ soll  übers Dreieck wirken

**Perspektive:**

- Insbesondere auch schon zum Zeitpunkt der „Festlegung der Mittel“, d.h. die Verarbeitung soll von Anfang an möglichst konform zu den DS-Grundsätzen gestaltet werden.

# 3. Art. 25 Abs. 1 DSGVO

**(1) – Datenschutz durch Technikgestaltung („privacy by design“)**

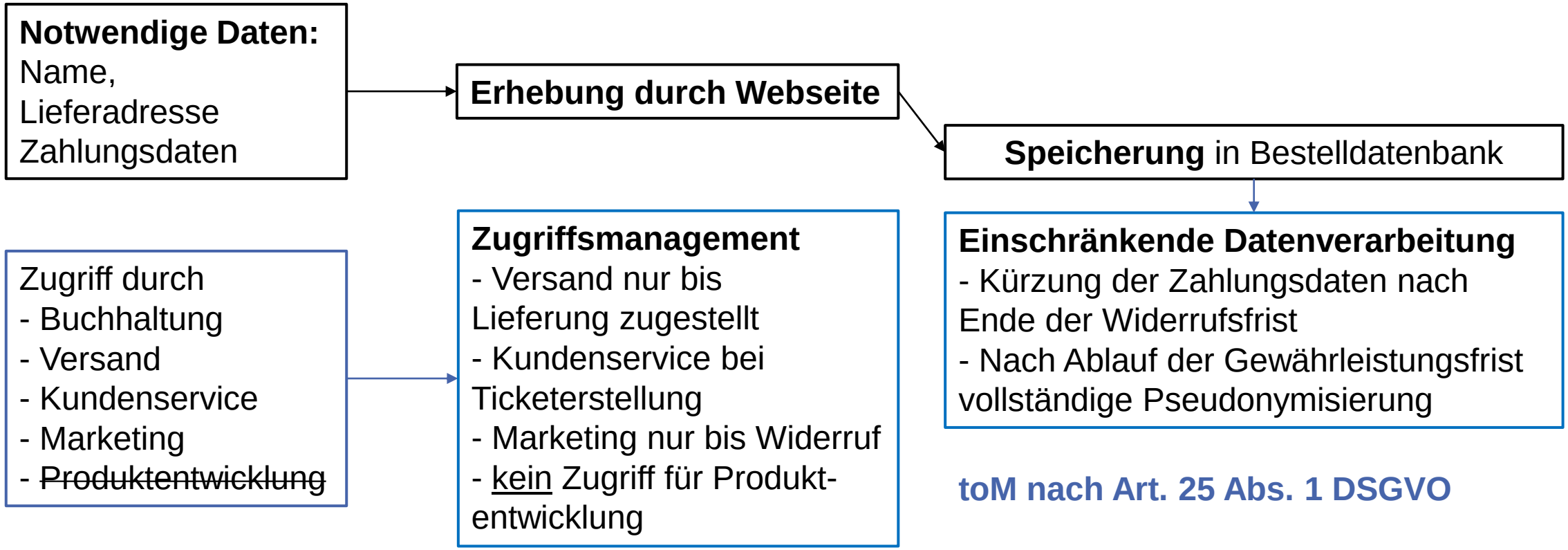
Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der [Modalitäten] der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft **der Verantwortliche** sowohl **zum Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch **zum Zeitpunkt der eigentlichen Verarbeitung** geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung, die dafür ausgelegt sind, **die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen** und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

## Beispiele

- Grundsatz der Datenminimierung (Zigarettenautomat)
- Grundsatz der Vertraulichkeit & Integrität: Schutz vor unbefugter Verarbeitung. (Durchführung der Verarbeitung durch möglichst wenige zuständige Mitarbeitende i.V.m. Zugriffsmanagement; internes Controlling zur Einhaltung)

# Fiktives Beispiel: Online-Bestellung

Zwecke der Verarbeitungen: Vertragserfüllung, Werbung, Steuerrechtliche Aufbewahrungspflichten (Art. 6 Abs. 1 b, c, f)




**toM nach Art. 25 Abs. 1 DSGVO**

# 3. Art. 25 Abs. 2 DSGVO

**(2) – Datenschutz durch datenschutzfreundliche Voreinstellungen („by default“)**

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass **durch Voreinstellung** nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck **erforderlich** ist, verarbeitet werden. [2]Diese Verpflichtung gilt für die **Menge** der erhobenen personenbezogenen Daten, den **Umfang** ihrer Verarbeitung, ihre **Speicherfrist** und ihre **Zugänglichkeit**. […]

**Datenschutz durch Voreinstellungen**

- „Grundsatz, dass ein Produkt oder Dienst für den Nutzer bereits ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten aufweisen soll.“
- Alles, **was zu weniger Datenschutz und mehr Datenverarbeitung** führt, ist vom Nutzer selbst aktiv einzuschalten und zu aktivieren (Opt-In).
- Z.b. bei Social-Media-Apps kein ungefragter Zugriff auf die auf dem Smartphone hinterlegten „Kontakte“

[Hartung in Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 24]

# 3. Art. 25 Abs. 2 DSGVO

**Fallbeispiel:** Smartphone-App „mit der Nutzer kurze Videoclips aufnehmen, bearbeiten und mit andern teilen können.“ war „so programmiert, dass bei der erstmaligen Installation grundsätzlich die globale Sichtbarkeit des Nutzerprofils und der vom Nutzer veröffentlichten Beiträge für alle anderen registrierten Nutzer **voreingestellt** ist. Die vom Nutzer veröffentlichten Beiträge können bei dieser Voreinstellung auch von nicht registrierten Nutzern aufgerufen werden.“ [1]

- Damit dürfte Verstoß gegen Art. 25 Abs. 2 DSGVO vorliegen

- Hier aber Begründung auch auf Art. 6 Abs. 1 lit b) (Vertragserfüllung) [i.V.m. Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit e) DSGVO)]; die standardmäßig eingestellte, weitergehende Verarbeitung sei jedenfalls **(auch) nicht zur Vertragserfüllung erforderlich**. [1]

- *D.h. Erlaubnistatbestand muss natürlich auch die Verarbeitung mit weiten Einstellungen abdecken (z.B. Einwilligung, berechtigtes Interesse) und dann muss aber trotzdem eine datenschutzfreundliche Voreinstellung erfolgen.*

[1] LG Berlin II (Zivilkammer 52), Urteil vom 23.06.2025 – 52 O 147/22, GRUR-RS 2025, 21288

# 4. Art. 32 DSGVO

**Artikel 32 DSGVO: <u>Sicherheit der Verarbeitung</u>**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen — Berücksichtigungskriterien

treffen der Verantwortliche **und** der Auftragsverarbeiter — Adressat

geeignete technische und organisatorische Maßnahmen, — Handlungsauftrag

<u>um</u> ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten; — Schutzzweck

# 4. Art. 32 DSGVO

diese Maßnahmen schließen unter anderem Folgendes ein:

a) die **Pseudonymisierung und Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der **Systeme und Dienste** im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;

d) ein Verfahren **zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Konkretisierung des Handlungsauftrags

(2) Bei der Beurteilung des **angemessenen Schutzniveaus** sind **insbesondere** die Risiken **zu berücksichtigen**, die mit der Verarbeitung – insbesondere durch **Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise **verarbeitet wurden** – verbunden sind.

Zu einem angemessenen Schutzniveau gehört insb.:

**Die Gewährleistung von Verfügbarkeit, Vertraulichkeit und Integrität von Daten**

# 4. Art. 32 DSGVO: Anwendungsbereich

**Anwendungsbereich, Normzweck: Art. 32 - „Sicherheit der Verarbeitung“**

- Art. 32 DS-DVO konkretisiert die allg. Aussage des Art. 24 DS-GVO hinsichtlich der technischen und organisatorischen Maßnahmen, zum Zwecke der **Datensicherheit**
- Die Verpflichtungen aus **Art. 32 DS-GVO** ergänzen jene aus **Art. 25 DS-GVO**
- Art. 32 DS-GVO will den Betroffenen insbesondere vor sicherheitsrelevanter **Vernichtung, Verlust und unbefugter Offenlegung bereits erhobener Daten** schützen.
- Zielt insbesondere auf Sicherheit von die Verarbeitung ausführenden „**Systemen und Diensten**“

# 4. Art. 32 DSGVO: Anwendungsbereich

**Abgrenzung des Schutzzwecks:**

- Art. 25 Abs. 1 DSGVO: „**Datenschutzgrundsätze wirksam umsetzen“**
  → Einhaltung der DS-Grundsätze und datenschutzfreundliche Voreinstellungen (v.a. Absicherung des Datenschutzes (keine unerlaubte Nutzung, Weitergabe der Daten)

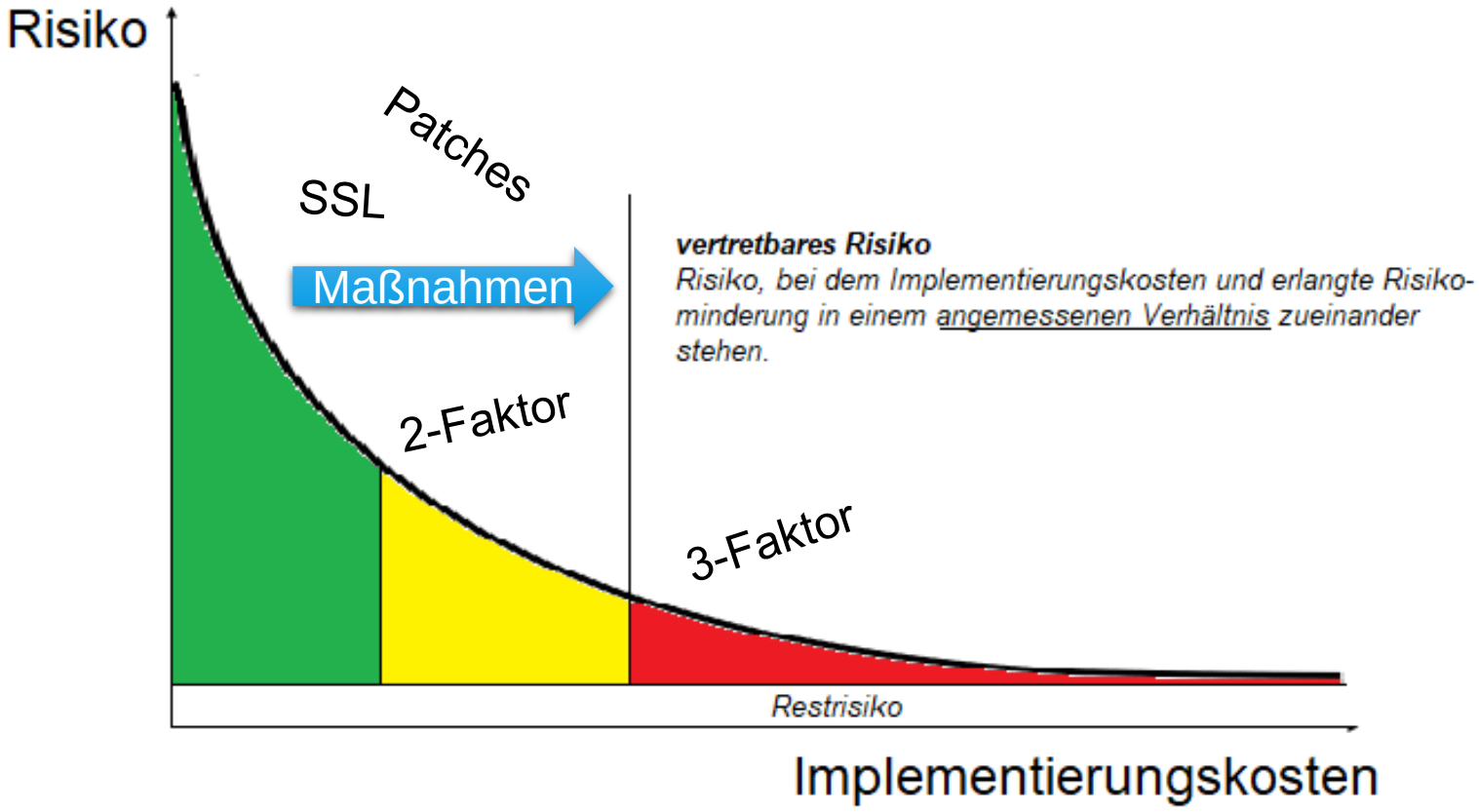
- Hier (Art. 32 Abs. 1 DSGVO) „**ein dem Risiko angemessenes Schutzniveau gewährleisten**“ **Sicherheitsniveau (uneinheitliche Übersetzung)**
  → Schutz i.S.d. der Datensicherheit, d.h. Schutz vor Angriffen, technischen Zwischenfällen, etc.

- Schutzgüter bleiben aber in jedem Fall „Rechte und Freiheiten“ natürlicher Personen

- **„Angemessenheit“** ist Ausdruck und Korrektiv der **Verhältnismäßigkeit** bei der Maßnahmenwahl;
- es ist eine Kosten-Nutzenabwägung zwischen den **Implementierungskosten** der Maßnahmen und der damit zu erreichenden **Risikoreduktion** vorzunehmen.

# 4. Art. 32 Abs. 1 DSGVO: Schutzzweck

**Schutzzweck: „ein dem Risiko angemessenes Schutzniveau“**



# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

diese Maßnahmen **schließen unter anderem Folgendes ein:**
[…]
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. […]

- Katalog verschiedener technischer und organisatorischer Maßnahmen (**Regelbeispiele**).
- Unterteilt in:
  - **Konkrete Maßnahmen**, wie die Pseudonymisierung/Verschlüsselung (Abs. 1 lit. a), und
  - **Abstrakte Maßnahmen**, die eher Zielvorgaben ähneln (lit. b und c).
  - **Verfahrensvorgaben** (lit d.)

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
a) die **Pseudonymisierung** und Verschlüsselung personenbezogener Daten;


- **Konkretisierende Maßnahmen: „Pseudonymisierung“**
- Verordnungsgeber sieht „**Pseudonymisierung**“ als Schlüsselelement für die Herstellung von **Verhältnismäßigkeit** zwischen Betroffenenrechten und Zielen des Verantwortlichen
- **„Pseudonymisierung“** (Methode), vgl. Art. 4 Nr. 5 DS-GVO, **siehe UE 5/15**
  - **Schutzziel nach Außen**: Sicherung der **Vertraulichkeit** gegen unbefugte **Offenlegung/Zugang**
  - **Schutzziel nach Innen (Art. 25 DSGVO):** Präventive Unterbindung einer unbefugten Weiterverarbeitung/Zusammenführung beim Verantwortlichen

**Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**
trifft der Verantwortliche […] geeignete technische und organisatorische Maßnahmen – **wie z. B. Pseudonymisierung** –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 <u>Sicherheit der Verarbeitung</u>**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
a) die Pseudonymisierung und **Verschlüsselung** personenbezogener Daten;

- **Konkretisierende Maßnahmen: „Verschlüsselung“**
- **„Verschlüsselung“** (Methode), besteht aus der *„Umwandlung eines Klartextes mittels eines kryptographischen Verfahrens (symmetrisch oder asymmetrisch) in eine nicht einfach interpretierbare Zeichenfolge“* [1]
  - **Schutzziele**: Sicherung der **<u>Integrität/Vertraulichkeit der Daten</u>**
  - **Entsprechende, ergänzende Auslegung des Art. 25 DSGVO:** Auch hier Verschlüsselung sinnvoll, um unzulässige Weiterverarbeitung zu unterbinden. Ggf. sogar vollständige nutzerbezogene Verschlüsselung, z.B. bei Messenger-Diensten, Fitnesstrackern

[1 vgl. hierzu Jandt in Buchner/Kühling DS-GVO Art. 32 Rn. 19 ff.]

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
b) die Fähigkeit, die **Vertraulichkeit**, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

**Konkretisierende Maßnahmen: „Vertraulichkeit“ von Systemen und Diensten**

- Die „**Vertraulichkeit**“ bezeichnet die **Geheimhaltung schützenswerter Informationen**
- **Maßnahmen** der **System- und Dienstbezogenen Umsetzung** des Gebots der Vertraulichkeit sind etwa:


Zutrittskontrolle


Zugangskontrolle
(Inkl. Verschlüsselung)

Zugriffskontrolle

O. Raabe; Vorlesung: Datenschutz durch Technik (ZAR/KIT)

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
b) die Fähigkeit, die Vertraulichkeit, **Integrität**, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

**Konkretisierende Maßnahmen: „Integrität“**

- Der **Schutz der Integrität** zielt darauf,  dass das System oder der Dienst die Manipulation von Daten verhindern kann
- **Maßnahmen** der **System- und Dienstbezogenen Umsetzung** des Gebots Integrität sind etwa
  - **Etablierung einer ständigen Eingabekontrolle/Systemüberwachung** zur Auswertung von Protokolldateien, können zum Schutz der Integrität beitragen
  - Einführung von Infrastrukturen für **fortgeschrittenen Signaturverfahren**

O. Raabe; Vorlesung: Datenschutz durch Technik (ZAR/KIT)

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
b) die Fähigkeit, die Vertraulichkeit, Integrität, **Verfügbarkeit** und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

**Konkretisierende Maßnahmen: „Verfügbarkeit“**

- Die Sicherung der **Verfügbarkeit** bezeichnet die Wahrscheinlichkeit, dass ein System eine geforderte Leistung tatsächlich erbringt, denn „*Daten sollen dauerhaft zugänglich und nutzbar sein*“ [1]
- **Maßnahmen** der **System- und Dienstbezogenen Umsetzung** des Gebots der Verfügbarkeit sind etwa
  - Die Einführung einer „Back-up-Vorsorge“, Mehrfachvorhaltung von Systemkomponenten
  - Systemgestaltung zur Erzeugung redundanten Datenkopien
  - Einführung einer USV, ESV (dient auch der Integrität)

[1 vgl. Karg in BeckOK DatenschutzR BDSG aF § 9 Rn. 46]

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

**Konkretisierende Maßnahmen: „Belastbarkeit“**

- Englische Fassung: „***resilience***“ - Der Begriff Resilienz leitet sich ab von dem lateinischen Wort resilire mit der Bedeutung **„zurückspringen**“.
- Kommt ursprünglich aus der Psychologie und meint dort: „die Fähigkeit einer Person […], erfolgreich mit belastenden Lebensumständen und negativen Folgen von Stress umzugehen.“ [1]
- Daneben in diversen anderen Disziplinen bekannt, u.a. Soziologie, Materialforschung, Klimaforschung, Informatik und Sicherheitsforschung

[1] *Wustmann*, Resilienz - Widerstandsfähigkeit von Kindern in Tageseinrichtungen fördern, 6. Aufl., Beiträge zur Bildungsqualität, Weinheim, Basel 2016, S. 18

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

„Resilienz [ist] die Fähigkeit eines Systems, […] unerwartete Ereignisse zu erkennen (detektive Maßnahmen) und die Datensicherheit möglichst zu erhalten (adaptive Maßnahmen) respektive schnellstmöglich und vollständig unter lernender Verbesserung wiederzuerlangen (regenerative Maßnahmen).“

- Detektive Maßnahmen
  - Fehler- oder Angriffserkennung: z.B. Hacker-Angriff (Intrusion-Detection, Honeypot)
- adaptive Maßnahmen
  - während des Angriffs: Zugriffssperren, Isolation der infizierten Komponente, Delegation der Aufgabe an andere Komponente
- Regenerative Maßnahmen:
  - im Datenschutzrecht nur im Rahmen von Verfügbarkeit (siehe Art. 32 lit c) und ggf. Selbstreparatur von geschädigten Daten: Integrität relevant.
  - nach dem Angriff: (maschinelles) Lernen für zukünftige Angriffe, um die Angriffserkennung und Abwehrmethoden zu verbessern.

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- **Konkretisierende Maßnahmen: „Belastbarkeit“**
- [M1]: Resilienz als **neues Schutzziel**: „die Fähigkeit eines Assets, Veränderungen in der Umgebung aufzunehmen und sich an diese anzupassen.“
- [M2]: **Resilienz ist ein Strategie** [2] zur Bewältigung von Störungen/Angriffen

- Für M2 spricht die Charakteristik der bisherigen Schutzziele (Arg.: Schutzziele beschreiben (binäre) Sollzustände von IT-Objekten, nicht dessen „Fähigkeiten“; Schutzziele können immer auch primäre Angriffsziele sein)

[1] vgl. Klaus et al., DuD 2021, 738 (739); [2] vgl. Hansen, Datenschutzrecht, DSGVO Art. 32 Rn. 36-46

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
c) die Fähigkeit, die **Verfügbarkeit der personenbezogenen Daten** und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;

**Konkretisierende Maßnahmen: „Wiederherstellung der Verfügbarkeit“**

- Explizite Benennung einer regenerativen Resilienzmaßnahme; dazu gehören u.a.:
- Redundanz von Datenbeständen (RAID-Systeme, insb. RAID 1: Mirroring oder RAID 5); auch auf entkoppelten Systemen
  - Notstromversorgung (USV, AEV)
  - Vertretungspläne für Personal
  - Im Einzelfall bewerten nach Schwere des Zwischenfalls, der Unumkehrbarkeit eintretender Schäden sowie der Sensibilität der Daten [1]

[1] vgl. auch Mantz in Sydow DS-GVO Art. 32 Rn 19

# 4. Art. 32 Abs. 1 Hs. 2 DSGVO

**Artikel 32 Sicherheit der Verarbeitung**
[..]diese Maßnahmen schließen unter anderem Folgendes ein:
d) ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. […]

**Konkretisierende Maßnahmen: „Überprüfung, Bewertung und Evaluierung“**

- Normativen **Leitidee**, dass erst die **regelmäßige Evaluation** der Maßnahmen das erforderliche Maß an Datensicherheit nachhaltig verbürgt.
  - Abs. 1 Hs. 2 lit. d DS-GVO ist insoweit Lex specialis zu Art. 24 Abs. 1 S. 2 DS-GVO
  - Sicherheitsrechtliches Pendant zum „Datenschutz durch Technik“ im **Vorfeld** der Verarbeitung (Art. 25 Abs. 2 DS-GVO)
  - Die **Nachsorge** erfolgt auf Grundlage externer oder interner **Prüfberichte** sowie Evaluierungen durch Betroffene und Nutzer (Fragebögen oder persönlichen Befragungen)
  - Auch fingierte Angriffe durch Dritte im Auftrag des Verantwortlichen, sog. **Penetrationstests** [1]
  - Keine normativen Vorgaben zum **Turnus** (Problem: Rechtssicherheit)

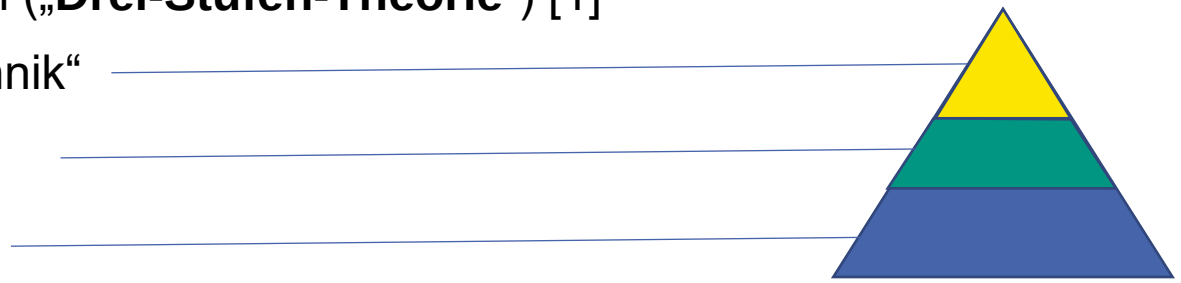
[1] vgl. auch Mantz in Sydow DS-GVO Art. 32 Rn 19

# Fallbeispiel: Online-Bestellung

- Zweck der Verarbeitung: Vertragserfüllung, Werbung, Steuerrechtliche Aufbewahrungspflichten (Art. 6 Abs. 1 b, c, f)

# Art. 32/25: Stand der Technik

- **Verweisungsbegriff in die Technikdomäne, „zu berücksichtigen“**
- **Abgrenzung** von verwandten Begriffen („**Drei-Stufen-Theorie**“) [1]
  - „Stand der Wissenschaft und Technik“
  - „Stand der Technik“
  - „Anerkannte Regeln der Technik“



- **Maßnahmen nach dem „Stand der Technik“ müssen**
  - technisch **tatsächlich realisierbar** sein (Eignung)
  - Dem **fortgeschrittenen Stand** der technischen Entwicklung entsprechen (Reifegrad)
  - **Anerkennung** durch **Fachleute**
  - **Bewährung** der Techniken in der **Praxis**
- **Idealerweise** in branchenspezifischen Leitfäden, Branchenspezifischen Sicherheitsstandards (B3S), u.ä. konkretisiert

[1] BVerfG, Beschluss vom 08.08.1978 - 2 BvL 8/77, Kalkar I

# Praxisbeispiel:

K kauft von V telefonisch ein Auto für 13.500€. Sie vereinbaren, dass der Kaufpreis auf Rechnung bezahlt werden sollte, welche der V dem K per Mail-Anhang zusenden wird. Um 11:44 erhält K die E-Mail mit der Original-Rechnung, um 11:46 erhält er eine weitere Mail mit einer manipulierten Rechnung. Cyberkriminelle hatten das Postfach des V übernommen und in der manipulierten Rechnung die Kontoverbindung ausgetauscht. K überweist den Kaufpreis auf das Konto der Kriminellen. Das E-Mail-Postfach des V war durch ein Passwort gesichert, welches angeblich alle zwei bis vier Wochen geändert wurde. 2FA oder Verschlüsselung waren nicht implementiert nicht.

V verlangt weiterhin Zahlung, K weigert sich. Wie ist zu entscheiden?

OLG Karlsruhe, Urteil vom 27.7.2023 – 19 U 83/22, MMR 2023, 761

# Praxisbeispiel:

# Praxisbeispiel: Lösung

**Datenschutz- und Zivilrecht:**

- durch die Zahlung an Kriminelle ist keine Erfüllung bei V eingetreten (§ 362 BGB); Zahlungsanspruch des V besteht fort.
- Fraglich, ob dem K ein SE-Anspruch in Höhe der 13.500€ gegen V zusteht, weil dieser seine Sicherungspflichten § 241 Abs. 2 BGB verletzt hat. Mit diesem Gegenanspruch könnte K „aufrechnen“ und müsste daher nicht zahlen.
- **Konturierung der Sicherungspflichten § 241 Abs. 2 BGB durch Art. 32 DSGVO**
  - Rechnung dürfte höchstwahrscheinlich personenbezogenes Datum darstellen (a.A. OLG Karlsruhe)
  - Art. 32 DSGVO nennt ausdrücklich „Verschlüsselung“, für E-Mails auch von DSK verlangt, soweit Risiko für Rechte und Freiheiten natürlicher Personen [1]
  - Außerdem dürfte **angemessenes Schutzniveau** 2-Faktor-Authentifizierung erfordern

- Zivilrechtliche IT-Sicherheitspflichten nach **§ 241 Abs. 2 BGB:** offen gelassen, BSI empfiehlt Verschlüsselung von E-Mails, gleichwohl im Rechtsverkehr kaum verbreitet

- Gegenanspruch des K somit laut OLG (-), mit DSGVO aber eher (+)

[1] DSK, https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf, Kap. 4.2.1

# 5. Datenschutz-, Datensicherheits- und IT-Sicherheitsrecht

- **Datenschutzrecht (DSGVO)**
  - Grundregelwerk zum Schutz des Rechts auf informationelle Selbstbestimmung


- **Datensicherheitsrecht (Art. 25/32 DSGVO)**
  - Verfügbarkeit, Vertraulichkeit, Integrität von **personenbezogenen Daten** sowie von verarbeitenden Systemen und Diensten (+ Belastbarkeit (Resilienz))

- **IT-Sicherheitsrecht (z.B. §§ 30, 31 BSIG)**
  - Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Diensten in **kritischen Infrastrukturen und digitalen  Diensten**

# 5. Datenschutz-, Datensicherheits- und IT-Sicherheitsrecht

## Datensicherheitsrecht (Art. 25/32 DSGVO)

- Verfügbarkeit, Vertraulichkeit, Integrität von personenbezogenen Daten sowie von verarbeitenden Systemen und Diensten (+ Belastbarkeit (Resilienz))
- Fokus: Vertraulichkeit personenbezogener Daten
- Schutzgüter: Individualrechte (insb. Recht auf informationelle Selbstbestimmung)

## IT-Sicherheitsrecht (z.B. §§ 8a, 8c BSIG)

- Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Diensten in kritischen Infrastrukturen und digitalen Diensten (nicht wie im (TD)DDG!)
- Fokus: Verfügbarkeit/Integrität von Diensten
- Schutzgüter: Insb. auch Gemeinschafts-rechtsgüter (z.B. sichere Energieversorgung, öffentliche Gesundheit, Wirtschaftsförderung)

# 5. Datenschutz-, Datensicherheits- und IT-Sicherheitsrecht

Verarbeitung von Gesundheitsdaten, Art. 4 Nr. 15 DSGVO

→ **Datensicherheit nach Art. 25/32 DSGVO**


Ab 30.000 vollstationären Fällen pro Jahr kritische Infrastruktur (Anhang 5 KritisV, Teil 3, Ziff. 1.1)

→ **IT-Sicherheit nach §§ 30, 31 BSIG**

**§ 31 Abs. 2 BSIG** Angriffserkennungssysteme

Möglicher Konflikt

**Datenschutz** der Mitarbeitenden

*Außerdem doppelte Melde- und Dokumentationspflichten*

# 5. Datenschutz-, Datensicherheits- und IT-Sicherheitsrecht

Andere IT-Sicherheitsgesetze (Auszug)

**Öffentliches Recht**

- „KRITIS-Recht“, §§ 30 f. BSIG
- § 165 TKG, Art. 6 ff. DORA, § 5c EnWG
- § 19 Abs. 4 TTDSG (Telemedien, insb. Webseiten)
- Art. 15 KI-VO
- Cyberresilience-Act, ProdSVO

**Zivilrecht**

- § 241 Abs. 2 BGB,
  Einzelfallabhängig, aber Mindestmaß an IT-Sicherheit immer erforderlich [1]
- Fehlende IT-Sicherheit (auch i.V.m. ausbleibenden Updates ist nun Sachmangel §§ 475b, 434 Abs. 3 BGB