

KI trifft Datenschutz

ARIC Session - 08.07.2025

Was ist Datenschutz?

Datenschutz schützt das Grundrecht jeder natürlichen Person, selbst zu bestimmen, ob, wann und wie ihre personenbezogenen Daten verarbeitet werden.

Personenbezogene Daten = alle Infos, die eine Person *direkt oder indirekt* identifizierbar machen (Art. 4 Nr. 1 DSGVO).

Ziele

- Wahrung der *informationellen Selbstbestimmung*
- Verhinderung von Diskriminierung, Identitätsdiebstahl, Profiling-Missbrauch

Wann dürfen personenbezogene Daten verarbeitet werden?

Art. 6 DSGVO → mind. eine Rechtsgrundlage nötig:

- **Einwilligung** – freiwillig, informiert, widerrufbar
- **Vertrag / vorvertragliche Maßnahme**
- **Rechtliche Verpflichtung**
- **Lebenswichtige Interessen**
- **Öffentliche Aufgabe / hoheitliche Gewalt**
- **Berechtigtes Interesse** (Interessenabwägung + Widerspruchsrecht)

Welche Rechte haben Betroffene?

Die DSGVO gibt jeder Person ein starkes Bündel von Rechten, um Kontrolle über ihre Daten zurückzuerlangen und verpflichtet Unternehmen, innerhalb von 30 Tagen (“unverzüglich”) transparent zu reagieren (Art. 12 Abs. 3).

Auskunft (Art. 15), Berichtigung (Art. 16), Löschung / „Recht auf Vergessenwerden“ (Art. 17), Einschränkung der Verarbeitung (Art. 18), Daten übertragbarkeit (Art. 20), Widerspruch (Art. 21), Keine allein-automatisierten Entscheidungen (Art. 22), Beschwerde & Schadenersatz (Art. 77 ff.)

Welche Pflichten haben Unternehmen?


Jedes KI- und Cloud-Projekt steht unter Beweislast: Nur wer Rechtsgrundlage, Technik- und Governance-Maßnahmen lückenlos nachweist, bleibt DSGVO- & KI-VO-konform.


- **Rechtsgrundlage & Zweck definieren (Art. 6)**
- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30)**
- **Privacy by Design / Default (Art. 25)**
- **Technische & organisatorische Maßnahmen (Art. 32)**
- **Datenschutzfolgenabschätzung (Art. 35 Abs. 3 lit. a–c)**

Show-Stopper? Cross-Border-Transfer


Transfer-Option	SCC + TIA	To-dos
Angemessenheitsbeschluss (z. B. EU-U.S. Data Privacy Framework, Schweiz, Japan, Südkorea)	Nein – Beschluss gilt als „angemessenes Schutzniveau“ (Art. 45 DSGVO).	Prüfen, ob Anbieter zertifiziert ist (DPF-List). Zweck, Umfang und Löschfristen dennoch dokumentieren.
Kein Beschluss (USA ohne DPF-Zert., Indien, China ...)	Ja	Zusätzliche technische Garantien (E2E-Verschlüsselung, EU-Keys etc.).
EU-Boundary / In-EU-Region	Nein – Daten verlassen den EWR nicht.	Region konfigurieren. Vertraglich fixieren, dass Logs + Supportdaten im EWR bleiben.

Beispiel Angemessenheitsbeschluss USA: www.dataprivacyframework.gov/list

**DATA PRIVACY
FRAMEWORK
PROGRAM**

Search  [Log In](#)

[Home](#) [Self-Certify](#) [Data Privacy Framework List](#) [Audiences](#) [About](#)






[FILTER RESULTS](#) [CLEAR FILTERS](#)

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#) [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [ALL](#)

[ACTIVE PARTICIPANTS](#) [INACTIVE PARTICIPANTS](#) [EXPORT LIST DATA](#)

Salesforce
San Francisco, CA

FRAMEWORK		STATUS	COVERED DATA
EU-U.S. Data Privacy Framework		Active	HR Data Non-HR Data
Swiss-U.S. Data Privacy Framework		Active	HR Data Non-HR Data
UK Extension to the EU-U.S. Data Privacy Framework		Active	HR Data Non-HR Data

+9 Covered Entities
[FULL PROFILE](#)

[Questions or Complaints](#)

Datenschutzbeauftragter

Art. 37 DSGVO

- Öffentliche Stelle – immer.
- Kerntätigkeit = **umfangreiche, regelmäßige Überwachung**
- Kerntätigkeit = **umfangreiche Verarbeitung besonderer Datenkategorien**

§ 38 BDSG (DE-Spezial)

- **≥ 20 Personen** verarbeiten regelmäßig automatisiert Daten, **ODER**
- eine **DSFA** ist vorgeschrieben, **ODER**
- Daten werden **geschäftsmäßig für Dritte** verarbeitet (Hosting, SaaS).

Wann ist eine DFSA erforderlich?

Immer dann, wenn die geplante Verarbeitung **voraussichtlich ein hohes Risiko** für Rechte und Freiheiten birgt.

Typische Trigger:

- **KI-Profiling oder Scoring** (Art. 35 Abs. 3 a)
- **Biometrie / Gesicht & Stimme** in großem Umfang (Abs. 3 b)
- **Systematische Überwachung öffentlicher Bereiche** (Abs. 3 c)
- In Deutschland zusätzlich jeder Vorgang auf der **DSK-Risikoliste** (z. B. KI-gestützter Kundensupport)

Was ist das Datenschutzrisiko
bei KI?

Was ist das Datenschutzrisiko bei KI?

- **Black-Box-Logik (darf es nicht geben):** Undurchsichtige Gewichtungen ⇒ schwer, Auskunft (Art. 15) oder Begründung zu liefern.
- **Zweckdrift & Datenhunger:** Nachtrainieren für neue Use-Cases verletzt Zweckbindung, Datenminimierung.
- **Unwiderrufliche Modell-Daten:**
 - **Finetuning** verschmilzt Eingaben mit Gewichten.
 - **Löschung/Berichtigung** (Art. 17 / 16) praktisch nicht mehr realisierbar.

3 Pfeiler datenschutzkonformer KI

Rechtsgrundlage + zweckgebundene Datenverarbeitung

(Art. 5 Abs. 1 lit. a–b & Art. 6)

Bevor Daten in eine Cloud- oder KI-Lösung fließen, muss eindeutig feststehen:

- Welcher Zweck? (z. B. Ticket-Zusammenfassung, Anomalie-Erkennung)
- Welche Rechtsgrundlage? (Einwilligung, Vertrag, berechtigtes Interesse usw.)
- Welche Daten sind dafür wirklich nötig? → Data-Minimization schon beim Design.

Ändert sich der Zweck, ist eine neue Legitimation nötig; „Vorratsdaten“ sind tabu.

Technische & organisatorische Schutzmaßnahmen (TOM)

(Art. 32)

Unternehmen müssen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten nach dem Stand der Technik garantieren, z. B.:

- Verschlüsselung (at rest & in transit) mit kundengemanagten Schlüsseln.
- Pseudonymisierung, Anonymisierung & RAG-Ansatz.
- Mandantentrennung, Zero-Trust-Netz, rollenbasiertes Zugriffsmanagement.
- Protokollierung, Monitoring & ein Incident-Response-Plan (72-h-Regel).

Transparenz, Betroffenenrechte & Rechenschaftspflicht

(Art. 12-22 & Art. 5 Abs. 2)

Betroffene müssen jederzeit nachvollziehen können, was mit ihren Daten geschieht. Unternehmen haben daher:

- Gut auffindbare Datenschutzhinweise (Kurzinformatio + Detail-Layer).
- Workflows für Auskunft, Löschung, Berichtigung, Widerspruch.
- Dokumentierte Datenschutz-Folgenabschätzungen (DSFA) bei hohem Risiko.
- Lückenlose Nachweise, dass alle Pflichten eingehalten werden.

Praxisbeispiel: Vornamenkorrektur

Ablauf

- Eingabe: Feld *Vorname* → Microsoft Azure Services (EU-Boundary)
- KI-Rückgabe „unklar“ ? → Fallback = Teil vor @ aus E-Mail (String-Split)

Datenschutz-Facts

- Daten bleiben **in EU-Region** ⇒ kein Drittlandtransfer
- Nur *Vorname* oder Mail-Alias ⇒ **Datenminimierung**
- Keine Modellweitergabe / -Training → Betroffenenrechte (Löschung, Berichtigung) sofort umsetzbar

Praxisbeispiel: Vornamenkorrektur

Rechtsgrundlage

- *Berechtigtes Interesse* Art. 6 (1) f DSGVO (Erwägungsgrund 39)

DSFA-Check

- Automatisierte Massenverarbeitung → **DSK-Risikolisteneintrag** ⇒ DSFA durchführen, Risiken dokumentieren

Transparenzhinweis

- Datenschutzerklärung & bei Datenauskunft

Legitimieren, schützen, erklären

Nur wer eine saubere Rechtsbasis hat, seine Daten technisch absichert und offenlegt, was passiert, nutzt KI- und Cloud-Services datenschutzkonform.

Wissenstipps & Links

- [KI Service Desk der Bundesnetzagentur >>](#)
- [Orientierungshilfen der Datenschutzkonferenz >>](#)
- [BfDI-Leitfaden KI & Datenschutz >>](#)
- [DFSA-Risikolisten >>](#)
- [DSGVO-Originaltext >>](#)

