Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

member of swissuniversities

AACSB ACCREDITED

KI-Compliance & Governance
Einsatz von KI-Tools im Unternehmen

SAS, 1. Durchführung

Prof. Dr. Bettina Schneider
Programmleiterin
Head FHNW Center for Digital Trust

01.11.2026



Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Seminar Tagesplan

AACSB ACCREDITED

1. Seminartag

09:00 Begrüssung (Bettina)

KI-Regulatorik – Überblick (Lukas): Verantwortlichkeiten im Kontext von KI; KI-Regulatorik – rechtliche Entwicklung in der Schweiz und der EU

Ergebnis: Big-Picture KI-Regulatorik

12:00 Mittagspause

KI-Regulatorik – Bezüge (Lukas): KI und Schweizer Datenschutzrecht; KI und Schweizer Arbeitsrecht

Übung: Reflexion über den derzeitigen Stand des Unternehmens.

Ergebnis: Standortbestimmung

16:45 Fragen und Abschluss

2. Seminartag

09:00 Begrüssung (Bettina)

Kriterien und strukturiertes Vorgehen (Susanne): Auswahl geeigneter KI-Tools aus vorhandenen Optionen

Ergebnis: Checkliste Beschaffung von KI-Tools

12:00 Mittagspause

Vorbereitung bei KI-Tool-Einsatz (Susanne): die Datenschutzfolgeabschätzung und KI-Compliance-Check

Ergebnis: Vorgehen zu KI-Risiko-Check bzw. KI-Compliance-Check

---

16:45 Fragen und Abschluss

3. Seminartag

09:00 Begrüssung (Bettina)

Technische Massnahmen beim Einsatz von KI-Tools (Bettina): Transparenz, Bias-Mitigation, Nachvollziehbarkeit

Ergebnis: Checkliste Technische Massnahmen

12:00 Mittagspause

Organisatorische Massnahmen beim Einsatz von KI-Tools (Susanne): Weisung für Mitarbeitende und Schulung

Übung: Weisung erarbeiten und Präsentation vorbereiten

Ergebnis: Gruppenpräsentation und Diskussion zur Weisung

16:30 Feedback und Abschluss

Gliederung

KI-Compliance & Governance: Einsatz von KI-Tools im Unternehmen

I. Willkommen

II. KI-Regulatorik: Schweiz, EU, Bezüge zu Datenschutz und Arbeitsrecht

III. Kriterien und Vorgehen: Auswahl KI-Tools aus vorhandenen Optionen

IV. Vorbereitung KI-Tool-Einsatz: DSFA und KI-Compliance-Check

V. Technische Massnahmen KI-Tool-Einsatz: Generell und KI-spezifisch

VI. Organisatorische Massnahmen KI-Tool-Einsatz: Weisung und Schulung

VII. Abschluss

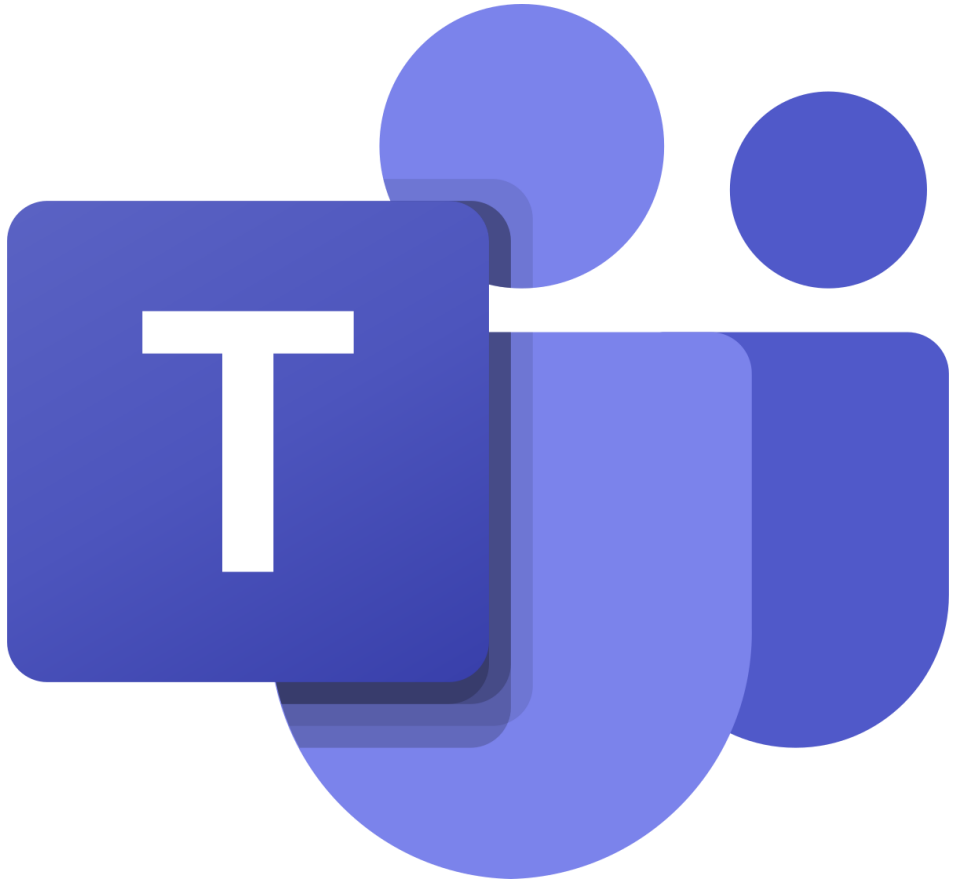
CAS als Weiterbildung-Meilenstein zum DAS

DAS Cybersecurity, AI & Data Governance (32 ECTS)
CAS AI powered CyberTech
CAS Cybersecurity & Information Risk Management
SAS KI-Compliance & Governance

Voraussetzung SAS-Abschluss

- **80% Anwesenheit**
- **Aktive Mitarbeit**
- **Präsentation**
  (Ergebnisse auf MS Teams abgelegt)

Lernplattform und Dokumente: MS Teams



Dozierenden-Team

Susanne Amrein
Leiterin Data Privacy Legal im Konzern der Basler Kantonalbank, Anwältin, Datenschutzexpertin und Auditor

E-Mail: *susanne.amrein@bkb.ch*
Phone: +41 61 266 23 06





Lukas Fässler
lic. iur. Rechtsanwalt

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b
6340 Baar

Telefon +41 41 727 60 80
Mobile +41 79 209 24 32
faessler@fsdz.ch



Prof. Dr. Bettina Schneider
Head of Competence Center Digital Trust
Institute vor Information Systems
bettina.schneider@fhnw.ch

www.digitaltrust-competence.ch

Regulatorik

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Gliederung

KI-Compliance & Governance: Einsatz von KI-Tools im Unternehmen

I. Das Europäische Datenrecht

II. Verantwortlichkeiten im Umgang mit Daten

III. Verantwortlichkeiten im Umgang mit dem Einsatz und Nutzung von KI

IV. Stand Schweiz

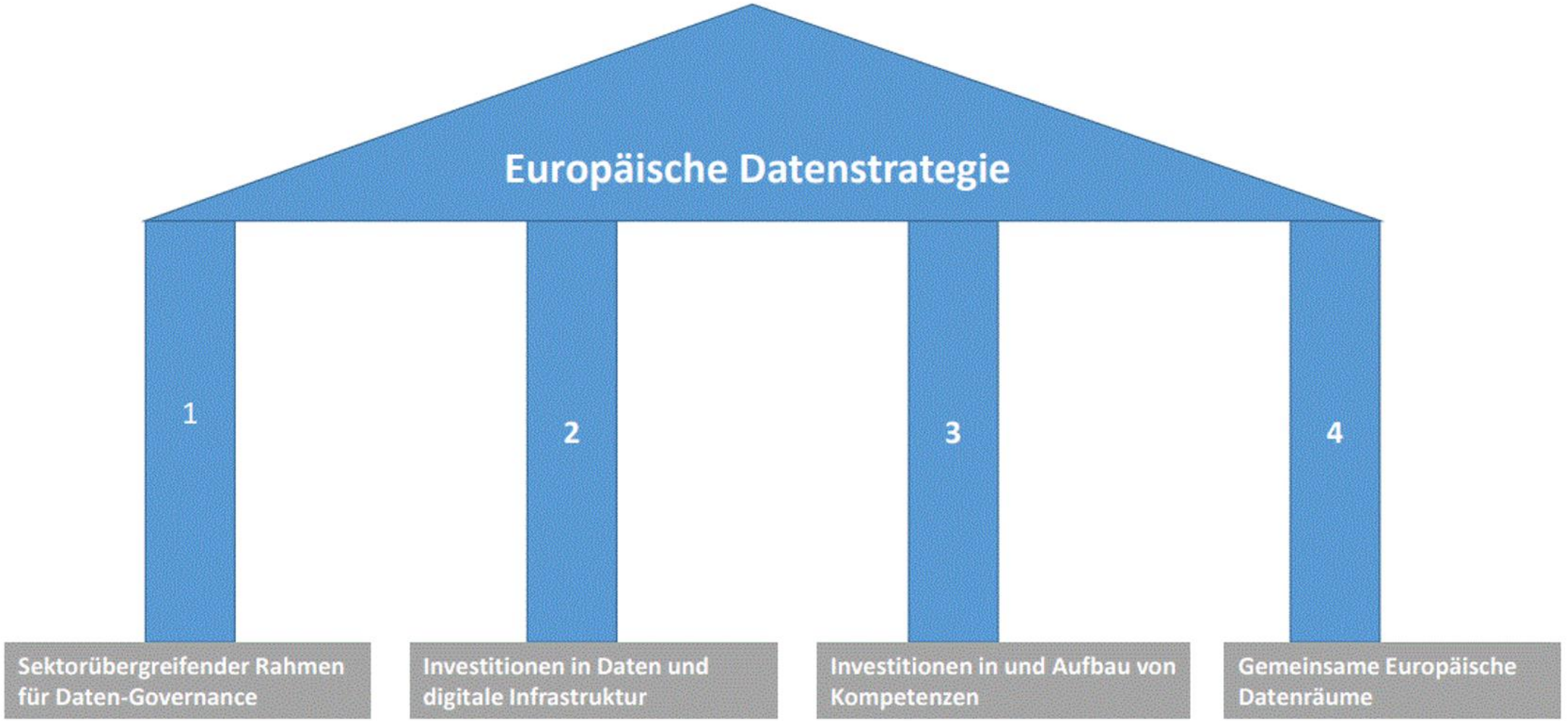
V. Datenschutzrecht und Arbeitsrecht

VI. Übung: Reflexion über den derzeitigen Stand des Unternehmens.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Das europäische Datenrecht

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026


Europäische Datenstrategie
1
2
3
4
Sektorübergreifender Rahmen für Daten-Governance
Investitionen in Daten und digitale Infrastruktur
Investitionen in und Aufbau von Kompetenzen
Gemeinsame Europäische Datenräume

DATENRECHT IM DIGITALEN ZEITALTER

Rechtliche Rahmenbedingungen für Daten in einer vernetzten Welt

WAS IST DATENRECHT?

Gesamtheit der Normen zum Zugang, zur Nutzung und zum Schutz von Daten – sowohl personenbezogener als auch nicht-personenbezogener Daten.

→ Querschnittsmaterie mit Bezügen u. a. zum Kartell-, Wettbewerbs- und Verbraucherschutzrecht. Datenschutzrecht (DSGVO)

DATENSCHUTZ ALS TEILGEBIET

Die Datenschutz-Grundverordnung **(DS-GVO)** hat das Datenschutzrecht seit ihrer Einführung im Jahr **2017** maßgeblich weiterentwickelt.

TECHNOLOGISCHER WANDEL

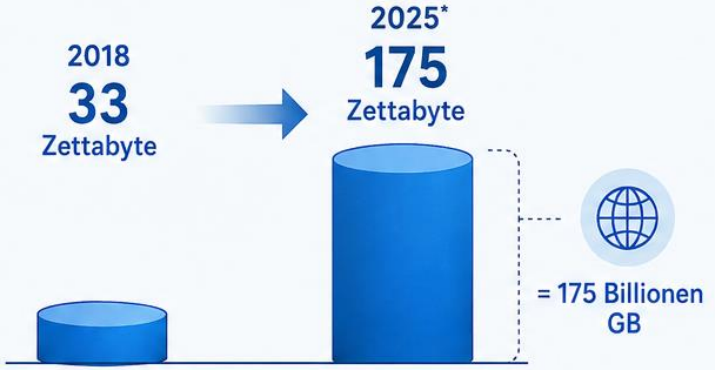
- Künstliche Intelligenz (KI) –
- Internet of Things (IoT) – Smartphones, Smartwatches, Smarthome-Assistenten
- Vernetzte Produkte erzeugen und verarbeiten immer größere Datenmengen. GPS-Daten, autonomes Fahren etc

DATEN ALS WIRTSCHAFTSFAKTOR

Daten besitzen ein erhebliches Wertschöpfungspotenzial, z. B. für die Weiterentwicklung vernetzter Produkte und deren Nutzung auf dem Sekundärmarkt. Open Government Data

EXPLOSIVES DATENWACHSTUM

Weltweit erzeugte Datenmenge



* Prognose

UNGENUTZTES POTENZIAL



Eine Studie im Auftrag der Europäischen Kommission zeigt:

Schätzungsweise **80 %** der Industriedaten bleiben gegenwärtig **ungenutzt**.

KERNAUSSAGE

Das Datenrecht muss mit dem rasanten technologischen Fortschritt und der wachsenden wirtschaftlichen Bedeutung von Daten Schritt halten.

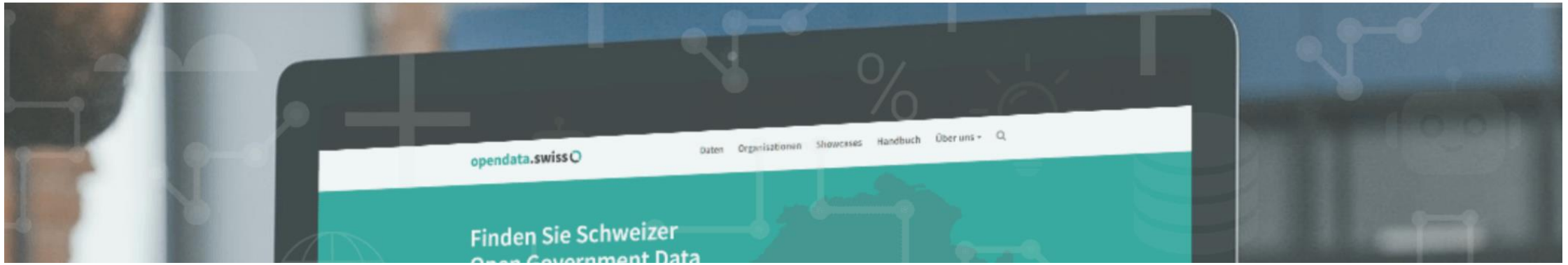
Open Government Data Schweiz



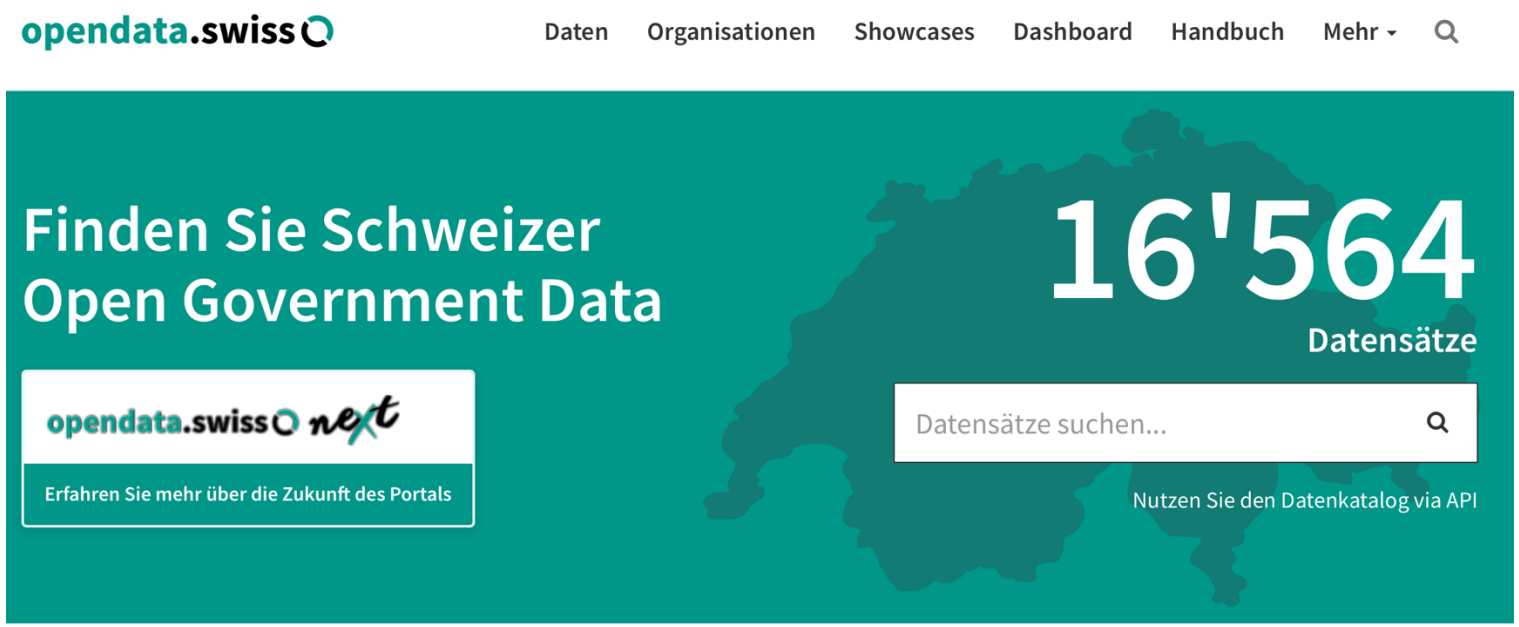
(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Das Portal opendata.swiss

Entdecken Sie opendata.swiss, das Portal für offene Verwaltungsdaten (OGD) der öffentlichen Verwaltung der Schweiz. Greifen Sie auf einen wahren Schatz an Datensätzen zu, die eine Vielzahl von Themen abdecken und von verschiedenen Organisationen bereitgestellt werden. Entdecken Sie unsere Ressourcen: Benutzerhandbuch, Showcase, Qualitäts-Dashboard und vieles mehr. Standardisierte Metadaten erleichtern die Suche und vereinfachen den Zugang zu Verwaltungsdaten.



(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026



Kategorien

Bevölkerung und Gesellschaft 2808

Bildung, Kultur und Sport 1777

Energie 725

Gesundheit 675

Internationale Themen 16

Justiz, Rechtssystem und öffentliche Sicherheit 409

Landwirtschaft, Fischerei, Forstwirtschaft und Nahrungsmittel 1566

Regierung und öffentlicher Sektor 2435

Regionen und Städte 3483

Umwelt 7228

Verkehr 1432

Vorläufige Daten 2

Wirtschaft und Finanzen 2128

Wissenschaft und Technologie 17

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026


EU-DIGITALSTRATEGIE: DATEN NUTZEN. WERTE SCHÜTZEN. ZUKUNFT GESTALTEN.
Die politischen Weichenstellungen der Europäischen Kommission für ein digitales Europa
AUSLÖSER: ERKENNTNIS DES MISSVERHÄLTNISSES
Die Europäische Kommission hat im Februar 2020 mit der Vorstellung der Digitalstrategie die politischen Weichen für einen „grundlegenden gesellschaftlichen Wandel" gestellt, der die fundamentale Bedeutung von Daten im wirtschaftlichen, sozialen und politischen Bereich neu definiert.
EIN UMFASSENDES STRATEGIEKONZEPT
Die Digitalstrategie ist ein umfassendes Strategiekonzept zur Gestaltung der digitalen Zukunft Europas und umfasst über 50 Schlüsselmaßnahmen.
DREI ZENTRALE ZIELE
Ziel ist es, vertrauenswürdige Technologien zu entwickeln und einzusetzen, die den Alltag der Unionsbürgerinnen und Unionsbürger verbessern – ohne europäische Werte zu unterminieren.
DIE DREI SÄULEN DER DIGITALSTRATEGIE
EIN DIGITALES EUROPA IM DIENSTE DER MENSCHEN
1. TECHNOLOGIE IM DIENST DER MENSCHEN
Vertrauenswürdige Technologien verbessern den Alltag und stärken demokratische Werte und Grundrechte.
2. FAIRE UND WETTBEWERBSFÄHIGE WIRTSCHAFT
Förderung einer innovativen Wirtschaft, Stärkung der Wettbewerbsfähigkeit und umfassender Verbraucherschutz.
3. OFFENE, DEMOKRATISCHE UND NACHHALTIGE GESELLSCHAFT
Digitale Technologien unterstützen eine offene Gesellschaft und tragen zur Wahrung und Stärkung von demokratischen Werten und Grundrechten bei.
MAßNAHMEN ZUR UMSETZUNG DER DIGITALSTRATEGIE
DIGITALE INFRASTRUKTUREN AUSBAUEN
Schnelle, sichere und nachhaltige Netze (z. B. 5G, Glasfaser, Cloud, High-Performance-Computing) als Grundlage für Innovation und Wachstum.
CYBERSICHERHEIT STÄRKEN
Schutz von Bürgerinnen und Bürgern, Unternehmen und öffentlicher Verwaltung vor digitalen Bedrohungen.
DIGITALE KOMPETENZEN FÖRDERN
Ausstattung aller Menschen mit den digitalen Fähigkeiten, die für Teilhabe, Bildung und den Arbeitsmarkt der Zukunft notwendig sind.
IM ZENTRUM: DIE MENSCHEN & EUROPÄISCHE WERTE
Technologischer Fortschritt im Einklang mit Freiheit, Demokratie, Rechtsstaatlichkeit und Nachhaltigkeit.
SCHATTENSEITEN DER DIGITALWIRTSCHAFT ADRESSIEREN
MARKTMACHT GROßER (TECH-)KONZERNE
Die übermäßige Marktmacht weniger Unternehmen soll eingedämmt und fairer Wettbewerb gewährleistet werden.
FEHLENDER ZUGANG ZU DATEN
Viele Marktteilnehmer haben keinen oder nur eingeschränkten Zugang zu Daten – eine gemeinsame Nutzung von Daten wird dadurch nahezu unmöglich.
ZIEL: EIN DIGITALES EUROPA, DAS INNOVATION FÖRDERT, WIRTSCHAFT STÄRKT UND GESELLSCHAFTLICHEN FORTSCHRITT NACHHALTIG SICHERT.

EUROPÄISCHE DATENSTRATEGIE

Ein gemeinsamer Binnenmarkt für Daten – für eine faire, innovative und wertebasierte Datenwirtschaft

DIE VISION

Die europäische Datenstrategie verschafft Europa eine „globale Führungsrolle in der datenagilen Wirtschaft".

DAS ZIEL

Bis 2025 eine europäische Datenwirtschaft schaffen, die effizient, innovativ und an europäischen Werten und Grundrechten ausgerichtet ist.

IM ZENTRUM: DER EUROPÄISCHE DATENRAUM

Ein gemeinsamer Binnenmarkt für Daten, in dem personenbezogene und nicht-personenbezogene Daten unter vordefinierten Bedingungen zugänglich gemacht und genutzt werden können.

DIE VIER SÄULEN DER DATENSTRATEGIE

1. **EIN RECHTSRAHMEN FÜR DATEN**
   Klare, kohärente und faire Regeln für den Zugang zu und die Nutzung von Daten im Binnenmarkt.
2. **INVESTITIONEN IN DATEN & INFRASTRUKTUREN**
   Aufbau sicherer, leistungsfähiger und interoperabler Dateninfrastrukturen und -dienste (u. a. Cloud, Edge).
3. **DATENVERFÜGBARKEIT & -NUTZUNG FÖRDERN**
   Faire Datenzugänge schaffen, Datenräume entwickeln und innovative Datennutzung in allen Sektoren ermöglichen.
4. **DATENKOMPETENZ & VERTRAUEN STÄRKEN**
   Digitale Kompetenzen ausbauen, Vertrauen in Daten stärken und hohe Cybersicherheitsstandards gewährleisten.

HERAUSFORDERUNGEN AUF DEM WEG ZUM EUROPÄISCHEN DATENRAUM

1. **FRAGMENTIERTER BINNENMARKT**
   Unterschiedliche oder fehlende mitgliedstaatliche Regelungen zum Zugang und zur Nutzung von Daten führen zu Rechtsunsicherheit und behindern einen funktionierenden Datenbinnenmarkt.
2. **UNTERSCHIEDLICHES NIVEAU AN CYBERSICHERHEIT**
   Verschiedene Sicherheitsstandards und -niveaus führen zu mangelndem Vertrauen in das freiwillige Teilen von Daten – zwischen Unternehmen und mit Behörden oder Privatpersonen.
3. **MANGELNDE VERFÜGBARKEIT VON DATEN**
   Obwohl immer mehr Daten erzeugt werden, stehen sie häufig nicht in ausreichendem Maß für die beteiligten (Wirtschafts-)Akteure zur Verfügung, insbesondere im Privatsektor.
4. **MACHTUNGLEICHGEWICHT**
   Große Plattformunternehmen verfügen über erhebliche Datenmengen und genießen Wettbewerbsvorteile gegenüber KMU und anderen Marktteilnehmern, die kaum Zugang zu diesen Daten haben.
5. **UNZUREICHENDE QUALITÄT & INTEROPERABILITÄT**
   Die Qualität und Interoperabilität verfügbarer Daten ist oft unzureichend und erschwert insbesondere die sektorübergreifende Nutzung von Daten erheblich.
6. **MANGELNDE DATENKOMPETENZ**
   Es fehlt an der erforderlichen Kompetenz zur Datenaufbereitung und -analyse. Ohne qualifizierte Fachkräfte bringt der Zugang zu Daten allein keinen Nutzen.

ZIEL: EIN EUROPÄISCHER DATENRAUM, DER WIRTSCHAFT STÄRKT, INNOVATION FÖRDERT UND EUROPÄISCHE WERTE SCHÜTZT.

WETTBEWERBSFÄHIGE WIRTSCHAFT | INNOVATION & DIGITALER FORTSCHRITT | OFFENE, DEMOKRATISCHE & NACHHALTIGE GESELLSCHAFT

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Datenrecht – Einführung und Systematisierung

Die wichtigsten Punkte auf einen Blick

Gewinnung von Übersicht

Versuch
einer
Systematisierung



1 Einführung in das Datenrecht

- Datenrecht als Querschnittsmaterie
- Einordnung in die EU-Digital- und Datenstrategie (2020)
- Rechtspolitische Grundlagen und Entwicklungslinien



2 Datenrecht im engeren Sinne

Systematisierung nach dem „Klammerprinzip" des BGB:

Allgemeiner Teil (horizontale Regelungen)
- Data Act
- Data Governance Act
- DS-GVO
- Digital Service Act (DAS)

Besonderer Teil (sektorale Regelungen)
- z. B. EHDS
- FiDAR

→ Ziel: Systematisierung und bessere Orientierung in der jungen Materie des Datenrechts

3 Datenrecht im weiteren Sinne: datenbasierte Geschäftsmodelle

Regulierung datenbasierter Geschäftsmodelle durch:

Produktbezogener Ansatz
z. B. KI-Verordnung, Cyber Resilience Act

Funktionsbezogener Ansatz
z. B. Digital Services Act, Digital Markets Act

Darstellung der Rechtsakte:

Anwendungsbereich → Rechte & Pflichten → Aufsicht & Durchsetzung → Zusammenfassung & Praxisfolgen

Leitgedanke: Verständliche **Systematisierung des europäischen Datenrechts** mit konkretem Nutzen für die juristische **Praxis.**

EHDS: Europäische Gesundheitsdatenraum **FiDAR**: Europäischer Finanzdatenraum **DSA: Digitaler Service Act**

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Datenrecht – Einführung und Systematisierung

Die wichtigsten Punkte auf einen Blick

Ziel

- ✓ Fundierte Einführung in das sich entwickelnde europäische Datenrecht
- ✓ Brücke zwischen Wissenschaft und Praxis
- ✓ Orientierung im komplexen Geflecht der europäischen Digital- und Datenrechtsakte Schweiz ?
- ✓ Fokus auf praxisrelevante Rechte, Pflichten, Aufsicht und Durchsetzung



1 Einführung in das Datenrecht

- Datenrecht als Querschnittsmaterie
- Einordnung in die EU-Digital- und Datenstrategie (2020)
- Rechtspolitische Grundlagen und Entwicklungslinien



2 Datenrecht im engeren Sinne

Systematisierung nach dem „Klammerprinzip" des BGB:

Allgemeiner Teil (horizontale Regelungen)	Besonderer Teil (sektorale Regelungen)
• Data Act • Data Governance Act • DS-GVO CH-DSG • Digital Service Act (DAS)	• z. B. EHDS • FiDAR

→ Ziel: Systematisierung und bessere Orientierung in der jungen Materie des Datenrechts

3 Datenrecht im weiteren Sinne: datenbasierte Geschäftsmodelle

Regulierung datenbasierter Geschäftsmodelle durch:

Produktbezogener Ansatz	Funktionsbezogener Ansatz
z. B. KI-Verordnung, Cyber Resilience Act	z. B. Digital Services Act, Digital Markets Act

Darstellung der Rechtsakte:

Anwendungsbereich → Rechte & Pflichten → Aufsicht & Durchsetzung → Zusammenfassung & Praxisfolgen

Leitgedanke: Verständliche **Systematisierung des europäischen Datenrechts** mit konkretem Nutzen für die juristische **Praxis.**

Governance-Grundsätze (**Sorgfalt & Verantwortung**)

Allgemeiner Teil

Europaweite horizontale Regelungen

Übersicht EU-Akte

- EU Data Act: Europäischer Rechtsrahmen für wettbewerbsfähige Datenwirtschaft (Verordnung EU 2023/2854)
- DAS Digitaler Service Act: Verordnung zur Schaffung einheitlicher europäischer Haftungs- und Sicherheits-Vorschriften für digitale Plattformen, Dienste und Produkte (Verordnung 2022/2065)
- DSGVO Datenschutz-Grundverordnung (Verordnung 2016/679)
-

EU Data Act

Verordnung (EU) 2023/2854

Amtsblatt
der Europäischen Union

DE
Reihe L

2023/2854

22.12.2023

VERORDNUNG (EU) 2023/2854 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Dezember 2023

über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([2]),

nach Stellungnahme des Ausschusses der Regionen ([3]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([4]),

in Erwägung nachstehender Gründe:

(1) In den letzten Jahren haben datengetriebene Technologien transformative Wirkung auf alle Wirtschaftssektoren gehabt. Insbesondere die rasche Verbreitung von Produkten, die mit dem Internet vernetzt sind, hat den Umfang

Artikel 50

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 12. September 2025.

Die Verpflichtung gemäß Artikel 3 Absatz 1 gilt für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12. September 2026 in Verkehr gebracht wurden.

Kapitel III gilt nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, die nach dem 12. September 2025 in Kraft treten.

Kapitel IV gilt für Verträge, die nach dem 12. September 2025 geschlossen wurden.

Kapitel IV gilt ab dem 12. September 2027 für Verträge, die am oder vor dem 12. September 2025 geschlossen wurden, sofern

a) sie unbefristet sind oder

b) ihre Geltungsdauer frühestens 10 Jahre nach dem 11. Januar 2024 endet.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Straßburg, am 13. Dezember 2023.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	P. NAVARRO RÍOS

EU Data Act

Europäischer Rechtsrahmen für eine wettbewerbsfähige Datenwirtschaft

- Seit 11. Januar 2024 in Kraft
- Erleichtert Zugang, Austausch und Nutzung von Daten in der EU
- Verbindliche Rechte für Dateninhaber, Nutzer und Dritte
- Faire Verträge, Cloud-Wechsel und Interoperabilität
- Erleichterter Datenzugang für öffentliche Stellen in Notlagen

Ergänzt den Data Governance Act (DGA)



Anwendungsbereich des EU Data Act

Personenbezogene und nicht personenbezogene Daten

Kap. 2 ·
Datenaustausch B2C & B2B

Kap. 3 ·
Gesetzliche Bereitstellungspflichten

Kap. 4 ·
Schutz vor missbräuchlichen Vertragsklauseln

Kap. 5 ·
Datenzugang öffentlicher Stellen in Notlagen

Kap. 6 ·
Wechsel zwischen Cloud-Diensten

Kap. 7 ·
Schutz vor unrechtmäßigem internationalem Datenzugriff



Räumlicher Anwendungsbereich

Marktortprinzip nach Art. 1 Abs. 3 Data Act

- Tätigkeit innerhalb der EU ist entscheidend – unabhängig vom Sitz der Person oder des Unternehmens.
- Erfasst sind vernetzte Produkte und verbundene Dienste, die im Unionsmarkt angeboten werden.
- Maßgeblich ist die erstmalige tatsächliche Bereitstellung eines Produkttyps oder einer Produktserie in der EU.
- Nicht entscheidend: Zeitpunkt von Vertragsschluss, Kauf oder Vertragserfüllung.

Entscheidend ist der Marktort, nicht die Niederlassung.



Data Act: Zeitlicher Anwendungsbereich

Art. 50 DA | gestaffelte Geltung

Station 1 –
12.09.2025

- Data Act grundsätzlich anwendbar
- Kapitel III: nur für Datenbereitstellungspflichten, die nach diesem Datum in Kraft treten
- Kapitel IV: gilt für Verträge, die nach diesem Datum geschlossen werden

Station 2 –
nach dem 12.09.2026

- Art. 3 Abs. 1 DA: Nutzerzugang zu Produkt- und Dienstdaten
- nur für danach in Verkehr gebrachte vernetzte Produkte und verbundene Dienste

Station 3 –
ab 12.09.2027

- Kapitel IV erfasst auch Altverträge (geschlossen bis 12.09.2025), wenn sie unbefristet sind oder frühestens 10 Jahre nach dem 11.01.2024 enden



Merke: allgemeine Anwendung 2025 – Produktpflichten 2026 – bestimmte Altverträge 2027



Sachlicher Anwendungsbereich des EU Data Act

Zentrale Begriffe und Datenkategorien

Erfasste Daten

- **Primärdaten** – automatisch erzeugte Rohdaten
- **Aufbereitete Daten** – kontextualisierte und nutzbar gemachte Daten
- **Metadaten** (Art. 2 Nr. 2 DA) – strukturierende Informationen über Daten
- **Produktdaten** (Art. 2 Nr. 15 DA) – durch vernetzte Produkte generiert und zugänglich
- **Verbundene Dienstdaten** (Art. 2 Nr. 16 DA) – Daten aus Nutzerhandlungen und Diensten
- **Ohne Weiteres verfügbare Daten** (Art. 2 Nr. 17 DA)
- **Teilweise: Daten virtueller Assistenten** (Art. 1 Abs. 4 DA)

Weitere Schlüsselbegriffe

- **Daten** (Art. 2 Nr. 1 DA) – digitale Darstellungen von Handlungen, Tatsachen oder Informationen
- **Vernetztes Produkt** (Art. 2 Nr. 5 DA) – Produkt, das Nutzungs- oder Umgebungsdaten erfasst und übermitteln kann
- **Verbundener Dienst** – Dienst, der Funktionen eines vernetzten Produkts ermöglicht oder erweitert
- **Virtueller Assistent** (Art. 2 Nr. 31 DA) – Software zur Verarbeitung von Aufträgen und Steuerung vernetzter Produkte
- **Datenverarbeitungsdienst** (Art. 2 Nr. 8 DA) – skalierbare Rechenressourcen auf Abruf

Nicht erfasst: Inhalte (Text, Audio, visuelle Darstellungen) und abgeleitete Daten.

Persönlicher Anwendungsbereich

Das Dreiecksverhältnis des Data Act



DATENINHABER

Verfügt über die relevanten Daten aus vernetzten Produkten oder verbundenen Diensten.



DATA ACT



NUTZER – Art. 2 Nr. 12 DA

Natürliche oder juristische Person, die ein vernetztes Produkt besitzt, nutzt oder verbundene Dienste in Anspruch nimmt.

DATENNUTZER

Erhält und nutzt Daten im Rahmen der gesetzlichen Voraussetzungen.

Nutzer können sein: Käufer/Eigentümer • Mieter • Leasingnehmer • Dienstnutzer • Unternehmen • öffentliche Stellen

Maßgeblich ist die tatsächliche Nutzung – nicht allein der Eigentumsstatus.



Geschäftsgeheimnisse im Data Act

Art. 4 Abs. 6 DA regelt den Schutz von Geschäftsgeheimnissen bei der Datenweitergabe – ein zentrales Thema für neue Mitarbeitende.



Begriffsbestimmung

Geschäftsgeheimnisse liegen vor, wenn Informationen **geheim**, von **kommerziellem Wert** und durch **angemessene Schutzmaßnahmen** gesichert sind (Art. 2 Nr. 18 DA i.V.m. Geschäftsgeheimnis-RL).



Beweislast & TOMs

Der **Dateninhaber** ermittelt die geschützten Daten. Die Offenlegung erfolgt nur unter **technischen und organisatorischen Maßnahmen (TOMs)**, die vertraglich zu vereinbaren sind.



Verweigerungsrecht

Bei Verstoß gegen TOMs oder drohendem schwerem Schaden kann der Dateninhaber die Weitergabe **verweigern oder aussetzen** – mit schriftlicher Begründung und Behördeninformation (Art. 4 Abs. 7, 8 DA).

Praxishinweis: Die EU-Kommission entwickelt nach Art. 41 DA Mustervertragsklauseln, die für die Gestaltung von Vertraulichkeitsvereinbarungen entscheidend sein werden.

DSA – Digitaler Service Act

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2022/2065 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 19. Oktober 2022

über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)

Artikel 93

Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Diese Verordnung gilt ab dem 17. Februar 2024.

Artikel 24 Absätze 2, 3 und 6, Artikel 33 Absätze 3 bis 6, Artikel 37 Absatz 7, Artikel 40 Absatz 13 und Kapitel IV Abschnitte 4, 5, und 6 gelten jedoch ab dem 16. November 2022.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Straßburg am 19. Oktober 2022.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	M. BEK

Das **Gesetz über digitale Dienste** (**GdD**; englisch *Digital Services Act, DSA*; französisch *Règlement sur les Services Numériques, RSN*) ist eine Verordnung der Europäischen Union, die einheitliche europäische Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte schuf.[1] Damit soll die Verbreitung illegaler Inhalte verhindert und Nutzer besser geschützt werden. Es ist mit dem Gesetz über digitale Märkte (*Digital Markets Act*, DMA) Teil eines Gesetzespakets über digitale Dienste in der Europäischen Union.[2]

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

KI-Verordnung

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1689

12.7.2024

VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juni 2024

zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Artikel 113

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 2. August 2026.

Jedoch:

a) Die Kapitel I und II gelten ab dem 2. Februar 2025;

b) Kapitel III Abschnitt 4, Kapitel V, Kapitel VII und Kapitel XII sowie Artikel 78 gelten ab dem 2. August 2025, mit Ausnahme des Artikels 101;

c) Artikel 6 Absatz 1 und die entsprechenden Pflichten gemäß dieser Verordnung gelten ab dem 2. August 2027.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 13. Juni 2024.

Im Namen des Europäischen Parlaments

Die Präsidentin

R. METSOLA

Im Namen des Rates

Der Präsident

M. MICHEL

Regluation von KI

Die **Verordnung über künstliche Intelligenz** (KI) (informell *KI-Verordnung*, *KI-VO*, englisch *AI Act* oder *EU AI Act*) ist ein Rechtsakt der Europäischen Union zur Regulierung von künstlicher Intelligenz. Die EU-Verordnung ist weltweit die erste derartige Festlegung harmonisierter Vorschriften zur umfassenden Regulation von KI.[1][2]

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Entstehungsgeschichte

Sie wurde ab 2019 ausgearbeitet, am 21. Mai 2024 von den 27 EU-Mitgliedsstaaten endgültig verabschiedet[3] und am 12. Juli desselben Jahres im Amtsblatt der Europäischen Union verkündet.[4] Offiziell in Kraft getreten ist sie zum 1. August 2024.[5] Gemäß Art. 113 der Verordnung gelten ihre Regelungen mit einigen Ausnahmen überwiegend seit dem 2. August 2026.[6]

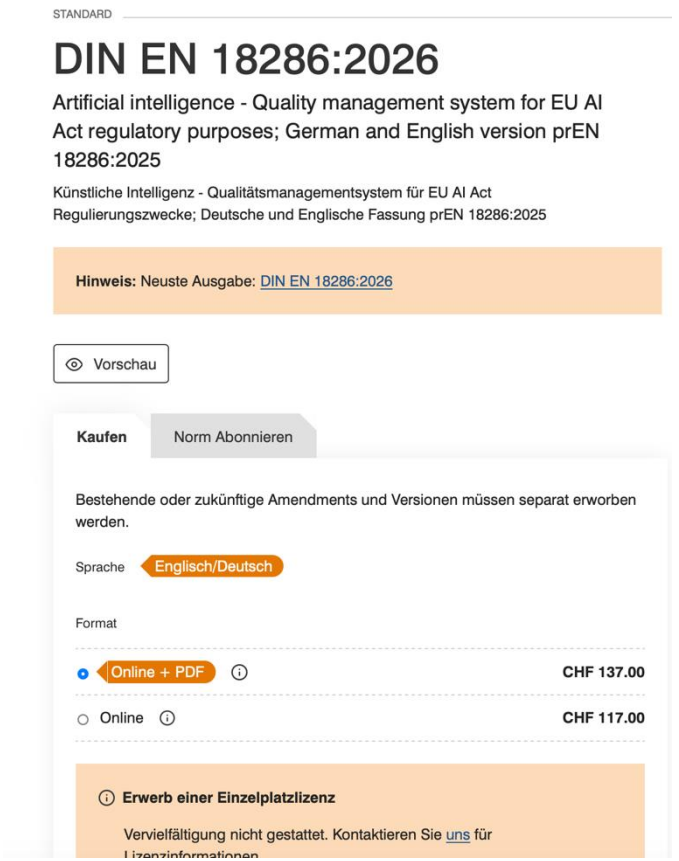
Die EU-Kommission beauftragt auf Grundlage der Verordnung (EU) Nr. 1025/2012 (Normungsverordnung) die europäischen Normungsorganisationen zur Entwicklung von harmonisierten Normen und gemeinsame Spezifikationen.[9]

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Begleitende Normierung

Mit dem Durchführungsbeschluss (EU) 2026/2274 der EU-Kommission vom 12. Oktober 2026 wurde die harmonisierte Nom *EN 18286:2026 Künstliche Intelligenz – Qualitätsmanagementsystem zu Regulierungszwecken im Rahmen der KI-Verordnung der EU* angenommen.[7]





Konformitätsbewertung

Allgemeines [Bearbeiten | Quelltext bearbeiten]

KI-Systeme sind Produkte, die in das Neue Konzept für die Produktkonformität in der Europäischen Union fallen[8]. Mit diesem Konzept werden regulatorische Vorgaben auf dem Gebiet der technischen Harmonisierung, der Normung und für das Inverkehrbringen von Produkten (EU-Wirtschaftsrecht) harmonisiert. Dazu werden, wie in dieser Verordnung, harmonisierte Vorschriften erlassen und mit einer Konformitätsbewertung dem spezifischen Produkt eine EU-Konformitätserklärung gegeben. Mit der EU-Konformitätserklärung wird die Einhaltung der harmonisierten Vorschriften bestätigt.

Zusätzliche Verordnung zur Marktüberwachung (2019/1020)

Mit der Verordnung (EU) 2019/1020 zur Marktüberwachung werden die staatenübergreifende Amtshilfe, Marktüberwachung und Kontrolle von KI-Systemen geregelt. Somit ist die Einhaltung der harmonisierten Vorschriften innerhalb der EU überprüfbar.

Da KI-Systeme in vielen Produkten enthalten sind, hat sich die Kommission die Befugnis zum Erlass delegierter Rechtsakte übertragen, um mit den delegierten Rechtsakten andere Produktvorschriften wie Verordnung (EU) 2023/1230 (EU-Maschinenverordnung) zu ändern. Dazu wird die Kommission von einem Ausschuss unterstützt (Komitologie).

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

CE-Kennzeichnung

Für Hochrisiko-KI-System ist eine CE-Kennzeichnung vorgeschrieben.[10]

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Haftung für fehlerhafte KI-Systeme

Die Haftung bei fehlerhaften KI-Systemen wird in der Richtlinie über Produkthaftung geregelt. Sie gilt für Produkte, die nach dem 9. Dezember 2026 in Verkehr gebracht oder in Betrieb genommen werden. Einen Vorschlag für eine spezielle Richtlinie über KI-Haftung hat die EU-Kommission im Oktober 2025 zurückgezogen.[11]

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Risikoeinstufung von KI-Technologien

Risikoeinstufung [Bearbeiten | Quelltext bearbeiten]

Die KI-Verordnung folgt einem weitgehend risikobasierten Ansatz. KI-Technologien, darunter auch generative KI (GenAI), werden in 4 verschiedene Risikoklassen eingeordnet:

1. KI-Systemen mit inakzeptablem Risiko
2. KI-Systeme mit hohem Risiko (Hochrisiko-KI-Systeme)
3. KI-Systeme mit begrenztem Risiko
4. KI-Systemen ohne Risiko.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Risikokategorien

Während KI-Systeme mit inakzeptablem Risiko nicht erlaubt sind (verbotene Praktiken, Art. 5 KI-VO), unterliegt der Betrieb von Hochrisiko-KI-Systemen besonderen rechtlichen Anforderungen (Art. 6ff KI-VO).

KI-Systeme ohne hohes Risiko sind grundsätzlich erlaubt. Bei bestimmten Einsatzarten und Interaktionsmöglichkeiten mit Endnutzern geht die KI-Verordnung jedoch von einem begrenzten und dennoch bestehenden Risiko aus, das durch entsprechende Informationen an die Nutzenden gemindert werden kann und soll. Um diese Risiken zu bewältigen, definiert die KI-VO bestimmte Transparenzpflichten, die sich an Anbieter und Betreiber richten (Art. 50 KI-VO).

KI-Systeme, die sich außerhalb der vorgenannten Risikoklassen bewegen (KI-Systeme ohne Risiko), unterliegen keiner gesonderten Beschränkung und können frei genutzt werden.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Verbotsvorgaben

Verbote [Bearbeiten | Quelltext bearbeiten]

Art. 5 verbietet Technologien mit einem inakzeptablen Risiko wie Social Scoring oder Teile von biometrischer Videoüberwachung bzw. Gesichtserkennung sowie automatisierter Emotionserkennung und subtiler Verhaltensbeeinflussung.[12] Für Strafverfolgungsbehörden, das Militär und Geheimdienste gibt es jedoch weitreichende Ausnahmen.[13]

Hochrisiko

Hochrisiko-KI-Systeme [Bearbeiten | Quelltext bearbeiten]

Definition der Hochrisiko-Systeme [Bearbeiten | Quelltext bearbeiten]

Zu den Hochrisiko-Systemen gehören:[14][15]

- Systeme, die biometrische Daten verarbeiten
- Systeme, die in der kritischen Infrastruktur zum Einsatz kommen
- Bewertung von Lernprozessen in Bildungseinrichtungen
- Zugangsprüfungen zur Universität und zu Hochschulen
- Bewerberauswahl, Beförderungen und Kündigungen im Arbeitsleben
- Anspruch auf Sozialhilfe
- Prüfung der Kreditwürdigkeit
- Risikobewertung und Preisbildung bei Lebens- und Krankenversicherungen
- Prognose von Rückfälligkeit bei Straftaten
- Einflussmöglichkeit auf Wahlen
- Einschätzung von Sicherheitsrisiken oder eines von Einzelnen ausgehenden Gesundheitsrisikos bei Migration, Asyl sowie bei Grenzkontrollen.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Betriebsanforderungen

Anforderungen an den Betrieb [Bearbeiten | Quelltext bearbeiten]

Anbieter von Hochrisiko-KI-Systemen müssen verschiedene Anforderungen erfüllen. Dazu zählt es u. a., ein Risikomanagementsystem einzurichten, Anforderungen an die Datenqualität zu erfüllen und menschliche Aufsicht über die KI sicherzustellen.[19] Ferner hat ein Konformitätsbewertungsverfahren nachzuweisen, dass die Anforderungen erfüllt werden. Nach Artikel 6 der EU-KI-Verordnung[20] gelten KI-Systeme im medizinischen Bereich, insbesondere in der Geburtshilfe und Pränataldiagnostik, als Hochrisiko-KI-Systeme. Betreiber müssen eine dauerhafte menschliche Aufsicht sicherstellen und über nachweisbare KI-Kompetenz verfügen. In der medizinrechtlichen Diskussion wird betont, dass Ärzte und Kliniken trotz automatisierter Entscheidungen weiterhin verantwortlich bleiben („Arzt als ultima ratio“).[21] Ist das Produkt nicht nur Hochrisiko-KI-System, sondern etwa auch Medizinprodukt, sind die Anforderungen an Hochrisiko-KI-Systeme im medizinprodukterechtlichen Konformitätsbewertungsverfahren mitzuprüfen.[22]

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Offenlegungspflichten

Betreiber von KI-Modellen mit allgemeinem Verwendungszweck müssen unter anderem offenlegen, mit welchen Daten die KI trainiert wurde, ob Internetseiten automatisch ausgelesen wurden und welche Maßnahmen zum Schutz von Urheberrechten ergriffen wurden. [23][24]

Kennzeichnungspflichten

Kennzeichnungspflichten [Bearbeiten | Quelltext bearbeiten]

Maschinenlesbare Kennzeichnung aller KI-Werke [Bearbeiten | Quelltext bearbeiten]

Anbieter von KI-Systemen müssen KI-generierte Bilder, Videos, Texte und Tonaufnahmen in maschinenlesbarer Form seit 2. August 2026 als künstlich kennzeichnen.

Generative KI

Eine **generative KI** (Künstliche Intelligenz) ist ein Computersystem, das selbstständig neue Inhalte wie Texte, Bilder, Musik, Videos oder Programmcode erzeugen kann. Wikipedia +1

Wie sie funktioniert

- **Trainingsdaten:** Das System wird mit riesigen Mengen an bestehenden Daten gefüttert (z. B. Bücher, Bilder, Websites).
- **Mustererkennung:** Die KI analysiert statistische Zusammenhänge, Grammatik, Stile oder Formen in diesen Daten.
- **Generierung über Prompts:** Nutzer geben einen Textbefehl (einen sogenannten *Prompt*) ein, woraufhin die KI basierend auf Wahrscheinlichkeiten eine völlig neue, eigenständige Antwort oder Kreation ausgibt. SAP +4

Was ist eine generative KI



https://ki-campus.org/lernangebote/videos/generative-ki-2-minuten-erklaert

Mögliche Kennzeichnungen

Artikel 50 der Verordnung, folgendermaßen geschehen:

Symbol	Wann zu verwenden	Anwendungsbeispiele
	**Grundlegendes Symbol** Wenn KI an der Erstellung von Deep-Fake-Inhalten (Bild, Audio, Video) oder veröffentlichtem Text beteiligt war	Deep-Fake-Video mit der Textbezeichnung „Stimmen generiert mit“, gefolgt vom Basissymbol
	**Vollständig KI-generiert** Wenn der gesamte Deep-Fake-Inhalt (Bild, Audio, Video) oder Text vollständig von KI generiert wird	Vollständig KI-generierte Deep-Fake-Videos mit Politikern oder fiktiven Ereignissen Vollständig KI-komponierte Musik oder Kunst
	**Teilweise KI-modifiziert** Vorhandene, von Menschen erstellte Inhalte wurden teilweise durch KI verändert	Ein Gesicht auf einem authentischen Foto wird mithilfe von KI gegen das Gesicht eines Politikers ausgetauscht

Abgesehen von den beispielhaften Icons der EU-Kommission gibt es bereits eine Vielzahl anderer Icons und Symbole die für die Deklarierung solcher Inhalte verwendet werden. Medienunternehmen wie der ORF nutzen diese Freiheit um zu ihrem Corporate Design passende Icons zu verwenden.

	**Beispiel für ein anderes mögliches Label** Allgemein für Werke die durch KI verändert und/oder erzeugt wurden.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Kennzeichnung von Deepfakes

Kennzeichnung von KI-Deepfakes [Bearbeiten | Quelltext bearbeiten]

Wer mithilfe von KI Deepfakes (laut Gesetz ein KI-Werk, das „einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde“) erstellt, muss diese bei Veröffentlichung seit 2. August 2026 entsprechend kennzeichnen; es sei denn, das KI-System wird nur privat verwendet. Ausnahmen gelten für die Strafverfolgung und für künstlerische oder satirische Werke.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

KI-Texte

Kennzeichnung von KI-Texten [Bearbeiten | Quelltext bearbeiten]

Wer mithilfe von KI Texte erzeugt oder verändert, die „über Angelegenheiten von öffentlichem Interesse“ informieren, muss dies seit 2. August 2026 offenlegen; es sei denn, das KI-System wird nur privat verwendet. Diese Kennzeichnungspflicht entfällt, wenn die Inhalte redaktionell geprüft bzw. überarbeitet wurden sowie einer redaktionellen Verantwortung unterliegen.

Weitere Transparenzpflichten

Weitere Transparenzpflichten [Bearbeiten | Quelltext bearbeiten]

Ebenso muss Nutzern stets klar sein, dass sie mit einem KI-System interagieren.[33] Mittels der Kennzeichnungs- und Transparenzpflicht soll laut dem österreichischen Rechtswissenschaftler Marlon Possard unter anderem eine Risikominimierung von Wahlbeeinflussung erzielt werden.[34]

Durchsetzung - Strafrahmen

Durchsetzung [Bearbeiten | Quelltext bearbeiten]

Der AI Act selbst droht sehr hohe Bußgelder an, wenn Unternehmen gegen ihn verstoßen. Artikel 99 sieht hier Strafen bis zu 7 Prozent des weltweiten Vorjahresumsatzes oder 35 Millionen Euro vor – dies ist deutlich mehr, als bei DSGVO-Verstößen drohen.[35] Außerdem ist die Schaffung eines Europäischen Gremiums für Künstliche Intelligenz (KI-Gremium)[36] vorgesehen, zur Durchsetzung sollen auf nationaler Ebene Behörden mit der Möglichkeit von Bußgeldern geschaffen werden.[37]

Anwendungsbereich (extraterritoriale Ausdehnung)

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für

a) Anbieter, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;

b) Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder in der Union befinden;

c) Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird;

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Gesetzgebung zu KI in der Schweiz

Nein, die Schweiz hat derzeit kein eigenes, übergreifendes KI-Gesetz. swissai.ch

Aktueller Stand und geplante Schritte

- **Kein horizontales Gesetz:** Die Schweiz verzichtet auf ein umfassendes, branchenübergreifendes KI-Gesetz nach dem Vorbild der EU (AI Act). swissai.ch
- **KI-Konvention des Europarats:** Der Bundesrat hat beschlossen, die völkerrechtliche KI-Konvention des Europarats zu ratifizieren. Schweizerische Vereinigu...
- **Vernehmlassungsvorlage:** Das Bundesamt für Justiz (BJ) erarbeitet bis Ende 2026 einen Gesetzesentwurf zur Umsetzung dieser Konvention, der sich vor allem mit Transparenz, Datenschutz, Nichtdiskriminierung und Aufsicht befassen wird. bk.admin.ch +1

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

KI-Konvention des Europarates

Die KI-Konvention des Europarates (*Rahmenübereinkommen über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit*, CETS-Nr. 225) ist der erste weltweit rechtsverbindliche völkerrechtliche Vertrag zum Thema Künstliche Intelligenz. www.coe.int +1

KI-Konvention des Europarates (2)

Die wichtigsten Fakten im Überblick

- **Verabschiedung:** Am 17. Mai 2024 wurde die Konvention vom Ministerkomitee des Europarates angenommen. www.coe.int
- **Ziel:** Schutz der Menschenrechte, der Demokratie und der Rechtsstaatlichkeit über den gesamten Lebenszyklus von KI-Systemen bei gleichzeitiger Förderung von Innovation. www.coe.int
- **Geltungsbereich:** Gilt sowohl für den Einsatz von KI im staatlichen bzw. öffentlichen Bereich als auch für private Akteure (mit gewissen Einschränkungen für die nationale Sicherheit). AlgorithmWatch CH +1
- **Unterzeichner:** Neben den Mitgliedstaaten des Europarates haben auch Staaten wie die USA, Israel und die Europäische Union die Konvention unterzeichnet. AlgorithmWatch CH +1
- **Inkrafttreten:** Tritt in Kraft, sobald fünf Staaten (davon mindestens drei Mitgliedstaaten des Europarates) das Abkommen ratifiziert haben. Bundesministerium der Ju...

Schweiz: Konvention unterzeichnet

Situation in der Schweiz

- **Unterzeichnung:** Die Schweiz hat die Konvention am 27. März 2025 durch Bundesrat Albert Rösti unterzeichnet.
- **Umsetzung:** Da die Vorgaben nicht direkt anwendbar sind, beauftragte der Bundesrat das EJPD, bis Ende 2026 eine entsprechende gesetzliche Grundlage für das Schweizer Recht auszuarbeiten. Swiss government +2

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Erwartete gesetzliche Rahmenbedingungen in Schweiz

1. Pflichten für Unternehmen aus der KI-Konvention

Die KI-Konvention des Europarates ist ein **völkerrechtliches Rahmenübereinkommen**. Das bedeutet, sie richtet sich primär an die Staaten (die Unterzeichner) und enthält Prinzipien, die diese in nationales Recht giessen müssen. AlgorithmWatch CH

Für private Unternehmen gelten die Pflichten daher **indirekt** – je nachdem, wie flexibel der jeweilige Staat die Regeln in Gesetze fasst. Die Konvention verlangt von den Staaten jedoch, dass auch im privaten Sektor folgende Kernprinzipien sichergestellt werden: AlgorithmWatch CH

- **Risiko- und Folgenabschätzungen:** Unternehmen müssen die Auswirkungen ihrer KI-Systeme auf Menschenrechte, Demokratie und Rechtsstaatlichkeit prüfen und bewerten. www.coe.int +1
- **Transparenz und Offenlegung:** Nutzer müssen wissen, wann sie mit einem KI-System interagieren oder wann Inhalte durch KI generiert wurden. Swiss government +1
- **Rechenschaftspflicht und Haftung:** Es muss klare Verantwortlichkeiten für Schäden oder Fehlfunktionen geben, die durch KI-Systeme verursacht werden. ResearchGate
- **Garantie menschlicher Aufsicht:** Bei kritischen Entscheidungen (z. B. im Personalwesen) muss sichergestellt sein, dass letztlich ein Mensch die Kontrolle behält und KI-Entscheidungen anfechtbar sind. Kompass Consulting & So...

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Aktueller Rechtsrahmen in der Schweiz

Welche Regeln gelten heute schon?

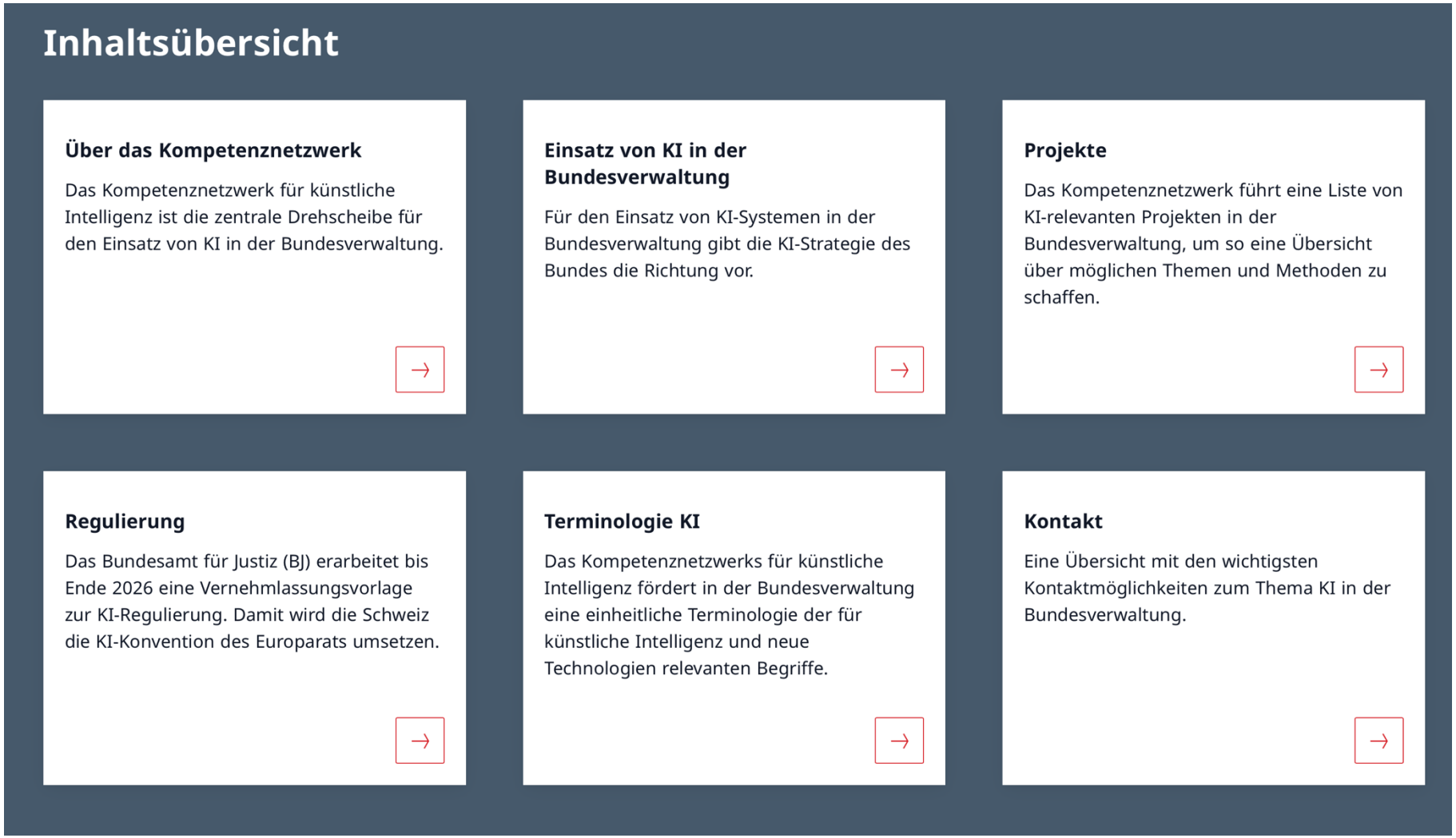
Wer in der Schweiz Künstliche Intelligenz nutzt, ist nicht rechtsfrei, sondern muss bestehende, technologieneutrale Gesetze einhalten: swissai.ch

- **Datenschutzgesetz (DSG):** Gilt laut dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) direkt für die Bearbeitung von Personendaten durch KI, inklusive Transparenzpflichten und Rechten auf menschliche Überprüfung von Entscheidungen. ODCUS
- **Lauterkeitsrecht:** Wer Kundschaft durch unkenntlich gemachte KI-Inhalte (z. B. Chatbots oder Deepfakes) täuscht, verstösst gegen das Gesetz gegen den unlauteren Wettbewerb. OVA Partner
- **Urheber- und Persönlichkeitsrechte:** Es gelten die allgemeinen Bestimmungen zu geistigem Eigentum und Schutz der Privatsphäre. Universität Basel +1
- **Sektorielle Vorgaben:** Spezifische Regeln für den Einsatz von KI werden je nach Branche (z. B. Medizin, Finanzsektor) direkt in den jeweiligen Spezialgesetzen angepasst. Schweizerische Vereinigu...

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Informationsplattform der Bundeskanzlei





https://www.bk.admin.ch/de/ki

Gesetzesentwurf über Kommunikationsplattformen und Suchmaschinen

Kommunikationsplattformen: Bundesrat will Jugendschutz ausbauen

Bern, 14.10.2026 — An seiner Sitzung vom 14. Oktober 2026 nahm der Bundesrat die Ergebnisse der Vernehmlassung des Gesetzes über Kommunikationsplattformen und Suchmaschinen zur Kenntnis und beauftragte das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK), bis Ende Juni 2027 eine Botschaft auszuarbeiten. Der Vorentwurf soll mit Jugendschutzmassnahmen ergänzt werden. Zudem soll das Meldeverfahren auf alle mutmasslich rechtswidrigen Inhalte ausgedehnt werden.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Ziele der Plattformregulierung

Die Ziele der Plattformregulierung

Die Bevölkerung informiert sich immer stärker über Kommunikationsplattformen und Suchmaschinen wie Google, Facebook und YouTube und bildet sich so ihre Meinung. Die Plattformen beeinflussen damit vermehrt die öffentliche Debatte. Mit dem neuen KomPG sollen die Rechte der Nutzerinnen und Nutzer gestärkt und die Anbieterinnen von Kommunikationsplattformen und Suchmaschinen zu mehr Transparenz verpflichtet werden.

Das Gesetz soll für sehr grosse Kommunikationsplattformen und Suchmaschinen gelten, dazu gehören auch KI-Suchmaschinen. Die Vorlage soll jedoch nicht auf kleinere Dienste ausgeweitet werden. Anbieterinnen von Kommunikationsplattformen sollen dazu verpflichtet werden, Nutzerinnen und Nutzern ein Verfahren zur Verfügung zu stellen, mit dem sie alle mutmasslich rechtswidrigen Inhalte unkompliziert melden können.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Jugendschutz verstärken

Neue Massnahmen zum Online-Jugendschutz

Der Bundesrat hält damit an der Vernehmlassungsvorlage fest, hat aber beschlossen, den Online-Jugendschutz deutlich auszubauen. So will er eine Risikobewertung und -minderung einführen. Die sehr grossen Kommunikationsplattformen und Suchmaschinen sollen analysieren müssen, inwiefern ihre Dienste Risiken für Minderjährige schaffen oder verstärken. Ausserdem müssen sie Massnahmen ergreifen, um diese Risiken zu reduzieren. So sollen Minderjährige die grossen Dienste sicherer nutzen können und es soll damit ihrem Recht auf Teilhabe am öffentlichen Diskurs Rechnung getragen werden. Zudem soll den Anbieterinnen untersagt werden, Minderjährigen Werbung auf Grundlage von Profiling auszuspielen, also aufgrund der Analyse ihres Online-Verhaltens und ihrer persönlichen Merkmale. Der Bundesrat entscheidet gestützt auf den Bericht zu den Postulaten 24.4480 Vara und 24.4592 Graf, ob und welche zusätzlichen Massnahmen im Bereich Jugendschutz in den rechtlichen Grundlagen zu verankern sind.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Botschaft bis Juni 2027

Der Bundesrat hat das UVEK beauftragt, auf Basis der Vernehmlassungsergebnisse bis im Juni 2027 eine Botschaft auszuarbeiten. Das UVEK bezieht das Eidgenössische Departement des Innern (EDI) bzw. das Bundesamt für Sozialversicherungen (BSV) in die Ausarbeitung der Jugendschutzbestimmungen ein.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Grundlagen des Datenschutzrechts

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Europäisches Datenschutzrecht

Datenschutz-Grundverordnung
DSGVO

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Artikel 99

Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Die **Datenschutz-Grundverordnung** (**DSGVO** oder **DS-GVO**; französisch *Règlement général sur la protection des données* RGPD, englisch *General Data Protection Regulation* GDPR) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Marktortprinzip

Art. 3 DSGVO

Räumlicher Anwendungsbereich

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

Schweizerisches Datenschutzrecht

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Bundesdatenschutzgesetz nDSG

- Bundesbehörden
- Private Unternehmen
- Bundesbeauftragte UN

26 kantonale Datenschutzgesetze

- Kantonale Verwaltungen
- Gemeinden
- Kantonale/kommunale Leistungserbringer (Spitäler, Gebäudeversicherungen etc.)

Bundesverfassung der Schweizerischen Eidgenossenschaft

vom 18. April 1999 (Stand am 3. März 2013)

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Bundesgesetz über den Datenschutz
(Datenschutzgesetz, DSG)

235.1

vom 25. September 2020 (Stand am 1. September 2023)

2. Kapitel: Allgemeine Bestimmungen
1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

c. *besonders schützenswerte Personendaten:*

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
3. genetische Daten,
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der sozialen Hilfe;

235.1

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020 (Stand am 1. September 2023)

---

2. Kapitel: Allgemeine Bestimmungen
1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

f. *Profiling:* jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

g. *Profiling mit hohem Risiko:* Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

Bearbeiten von Personendaten

Auch insbesondere für die Frage der Nutzung von KI-Werkzeugen massgeblich

d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

Bundesgesetz über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020 (Stand am 1. September 2023)

2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

j. *Verantwortlicher:* private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;

Art. 6 Grundsätze

[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Mass-

Treuepflichten des Arbeitnehmers auch bezüglich Datenschutz und Datensicherheit (und damit auch für den KI-Einsatz)

Art. 321*a*

II. Sorgfalts- und Treuepflicht

[1] Der Arbeitnehmer hat die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren.

[2] Er hat Maschinen, Arbeitsgeräte, technische Einrichtungen und Anlagen sowie Fahrzeuge des Arbeitgebers fachgerecht zu bedienen und diese sowie Material, die ihm zur Ausführung der Arbeit zur Verfügung gestellt werden, sorgfältig zu behandeln.

[3] Während der Dauer des Arbeitsverhältnisses darf der Arbeitnehmer keine Arbeit gegen Entgelt für einen Dritten leisten, soweit er dadurch seine Treuepflicht verletzt, insbesondere den Arbeitgeber konkurrenziert.

[4] Der Arbeitnehmer darf geheim zu haltende Tatsachen, wie namentlich Fabrikations- und Geschäftsgeheimnisse, von denen er im Dienst des Arbeitgebers Kenntnis erlangt, während des Arbeitsverhältnisses nicht verwerten oder anderen mitteilen; auch nach dessen Beendigung bleibt er zur Verschwiegenheit verpflichtet, soweit es zur Wahrung der berechtigten Interessen des Arbeitgebers erforderlich ist.

Ausdrückliche Einwilligung

Zulässigkeit der Bearbeitung von Personendaten

Art. 31 Rechtfertigungsgründe

[1] Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

[2] Ein überwiegendes Interesse des Verantwortlichen fällt insbesondere in folgenden Fällen in Betracht:

a. Der Verantwortliche bearbeitet die Personendaten über die Vertragspartnerin oder den Vertragspartner in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags.

Informationspflicht

- **Gesetzliche Grundlage**
- **Ausdrückliche Einwilligung**
- **Überwiegendes öffentliches Interesse**
- **Überwiegendes privates Interesse -> Abschluss oder Abwicklung Vertrag**

Bundesgesetz über den Datenschutz
(Datenschutzgesetz, DSG)

Art. 4 §11 DSGVO / Art. 6 Abs. 6 nDSG

vom 25. September 2020

Art. 6 Grundsätze

6 Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

7 Die Einwilligung muss ausdrücklich erfolgen für:

a. die Bearbeitung von besonders schützenswerten Personendaten;

b. ein Profiling mit hohem Risiko durch eine private Person; oder

c. ein Profiling durch ein Bundesorgan.

Einführung

Verantwortlicher

- Unternehmen
- Organisationen oder
- Privatpersonen,

die Personendaten besitzen und bearbeiten

Auftragsdatenverarbeiter

- ADV bei gleichem DS-Niveau
- SCC bei ungleichem DS-Niveau

Sorgfaltspflichten und Verantwortung

• VR	**717 und 754 OR**	Beweislastumkehr
• GL	754 OR	Beweislastumkehr
• Mitarbeitende	321a OR	Treuepflicht

Personendaten

Bearbeitung

Verhältnismässigkeit
Rechtsmässigkeit
Treu und Glauben
Zweckmässigkeit
Privacy by Default
Privacy by Design

Kategorien

- Personendaten (PD)
- Besonders schützenswerte PD
- Profilingdaten
- Profilingdaten mit besonderem Risiko

Internes Kontrollsystem IKS

- Bearbeitungsverzeichnis
- Datenschutzfolgeabschätzung
- TOMs
- ADV oder SCC
- DS-Bestimmungen (Online)

Betroffene

Rechte Betroffener

- Auskunftsrecht
- Berichtigungsrecht
- Löschungsrecht
- Herausgabe
- Rechte bei automatisierter Bearbeitung
- Benachrichtigungsrecht (data breach)

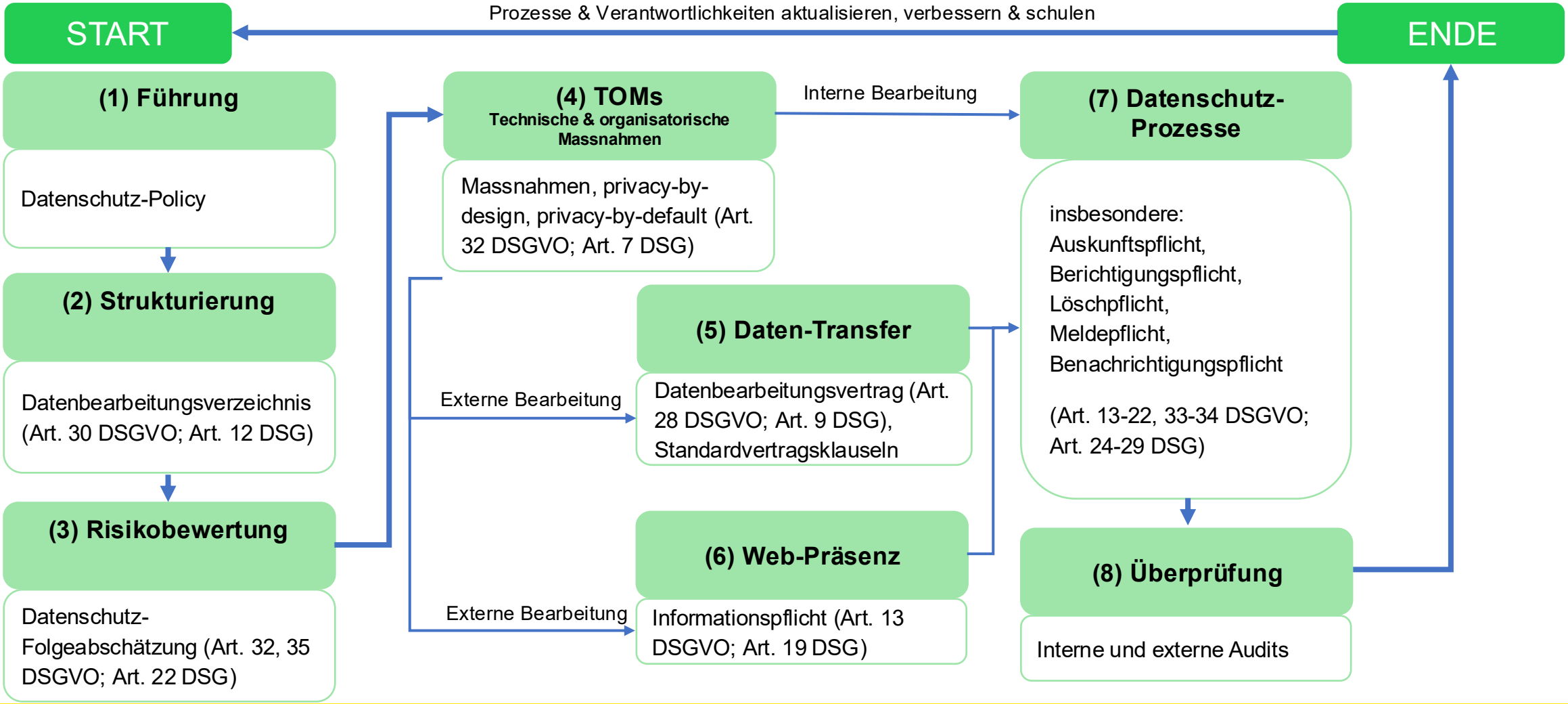
Datenschutz-Prozesse

Rechtfertigungsgründe

- Gesetzliche Grundlage
- Einwilligung
- Überwiegendes öffentliches Interesse
- Überwiegendes privates Interesse

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Datenschutz-Compliance – Die Roadmap



(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Sorgfaltspflichten der Führungskräfte

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

717 OR

VR-Mitglieder ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren müssen.

Das erforderliche Mass an Sorgfalt wird objektiv beurteilt und richtet sich danach, was von einem vernünftigen und gewissenhaften Menschen unter gleichen Umständen erwartet werden kann.

Eine Verletzung dieser Pflicht kann zur persönlichen Haftung des VR-Mitglieds führen, wenn dadurch ein kausaler Schaden entsteht.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

754 OR

Art. 754[645]

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

[1] Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.

[2] Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Beweislastumkehr zulasten der Führungskräfte

321a OR

Art. 321*a*

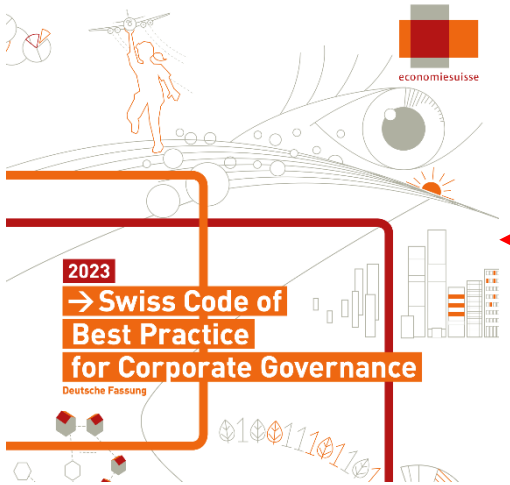
II. Sorgfalts- und Treuepflicht

[1] Der Arbeitnehmer hat die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren.

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026

Internes Kontrollsystem IKS

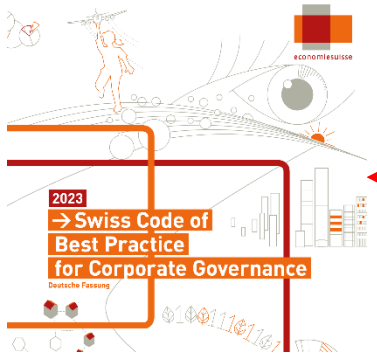
Im schweizerischen Obligationenrecht (OR) ist die Pflicht zur Führung eines internen Kontrollsystems (IKS) in Artikel 728a OR für Aktiengesellschaften verankert, die einer ordentlichen Revision unterliegen. Diese Vorschrift besagt, dass die Revisionsstelle im Rahmen ihrer Prüfung bestätigen muss, dass ein IKS existiert, und dass es den Geschäftsrisiken und der Tätigkeit des Unternehmens angepasst ist.



Internes Kontrollsystem IKS (2)

Der Kern der gesetzlichen Verpflichtung

- **Artikel 728a OR**: legt fest, dass die Revisionsstelle die Existenz eines internen Kontrollsystems zu prüfen hat.
- Dies betrifft nur Unternehmen, die zu einer ordentlichen Revision verpflichtet sind.
- Die Prüfung konzentriert sich auf die Existenz des IKS, also darauf, dass es dokumentiert, den Risiken angepasst und bekannt ist sowie tatsächlich angewendet wird.



Was das IKS leisten soll

- Das IKS dient dazu, die Zuverlässigkeit der Finanzberichterstattung sicherzustellen und Fehldarstellungen zu vermeiden.
- Es ist ein wesentlicher Beitrag zum Risikomanagement, da es Schwachstellen aufdeckt und eine wirksame, wiederkehrende Kontrolle ermöglicht.
- Das IKS soll einen Beitrag zur Sicherheit, Ordnungsmässigkeit und Wirtschaftlichkeit der Unternehmensprozesse leisten.

https://backend-api.economiesuisse.ch//sites/default/files/nn_migration/swisscode_d_web_1.pdf

(c) FSDZ Rechtsanwälte & Notariat AG, Baar 2026



economiesuisse

Umgang mit Risiken, Compliance und Finanzüberwachung (internes Kontrollsystem)

26

Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes internes Kontrollsystem, welches Risikomanagement, Compliance und Finanzüberwachung umfasst.

- Das interne Kontrollsystem dient dem Ziel, die Effektivität und die Effizienz der Geschäftstätigkeit (Operations), die Gesetzes- und Normenkonformität (Compliance) sowie die Verlässlichkeit der finanziellen und nichtfinanziellen Berichterstattung (Reporting) sicherzustellen.
- Das operative Management und die es unterstützenden Funktionen sorgen dafür, dass die Kontrollen gemäss den Vorgaben des Verwaltungsrats umgesetzt werden und dass sie wirksam sind.
- Die Ausgestaltung des internen Kontrollsystems hat der Grösse, der Komplexität und dem Risikoprofil des Unternehmens Rechnung zu tragen.

Risikomanagement

27

Das Unternehmen verfügt über ein angemessenes Risikomanagement. Der Verwaltungsrat nimmt eine regelmässige Risikobeurteilung vor.

- Das Risikomanagement umfasst namentlich strategische, operationelle, rechtliche und finanzielle Risiken sowie Marktrisiken bzw. Risiken für die Reputation des Unternehmens.
- Der Verwaltungsrat nimmt mindestens einmal jährlich eine Risikobeurteilung vor und berücksichtigt deren Ergebnis für seine Leitungs- und Aufsichtsaufgaben sowie für die Weiterentwicklung des internen Kontrollsystems.

Compliance und verantwortungsvolles Handeln

28

Der Verwaltungsrat ist dafür besorgt, dass das Unternehmen insgesamt Gesetze und interne Normen einhält (Compliance) und auch darüber hinaus verantwortungsvoll handelt.

- Der Verwaltungsrat ist im Rahmen seiner Oberaufsicht dafür besorgt, dass nicht nur seine Mitglieder, sondern das Unternehmen insgesamt, inklusive Management und Mitarbeitende, die Gesetze und internen Normen einhalten (Compliance) und dass auch darüber hinaus verantwortungsvoll gehandelt wird.
- Der Verwaltungsrat organisiert die Compliance nach den Besonderheiten des Unternehmens und erlässt geeignete Verhaltensrichtlinien. Er orientiert sich dabei an anerkannten Best-Practice-Regeln und beachtet die wichtige Rolle finanzieller wie nichtfinanzieller Anreize für Mitarbeitende und deren Vorgesetzte.[3]
- Die Geschäftsleitung trifft Massnahmen zur Einhaltung der Gesetze und internen Normen sowie für ein integres Geschäftsgebaren im Unternehmensalltag. Sie gewährt hierfür die erforderlichen personellen und finanziellen Ressourcen.


Minimalstandard zur Verbesserung
der IKT-Resilienz
https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Sanktionen nach DSGVO

Aufsichtsbehörden in EU-Ländern

- **Direktes Sanktionierungsrecht** gegenüber UN
- Katalog von Sanktionen

(Art. 58 § 2 DSGVO)

- Mahnung
- Verwarnung
- Förmliche Bekanntmachung der UN und des Verstosses
- Vorübergehende Beschränkung der Datenbearbeitung
- Dauerhafte Beschränkung der Datenbearbeitung
- **Geldbussen** von bis zu € 20 Mio oder 4% des weltweiten Jahresumsatzes
- Weitergehender Schaden (Schadenersatz und Zinsen) aus einem Gerichtsverfahren bleibt zusätzlich vorbehalten.

235.1

Bundesgesetz über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020 (Stand am 1. September 2023)

8. Kapitel: Strafbestimmungen

Art. 60 Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

1 Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;

b. die es vorsätzlich unterlassen:

1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder
2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

2 Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoss gegen Artikel 49 Absatz 3 dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

235.1

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020 (Stand am 1. September 2023)

Art. 61 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

a. unter Verstoss gegen Artikel 16 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 17 erfüllt sind, Personendaten ins Ausland bekanntgeben;

b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 9 Absätze 1 und 2 erfüllt sind;

c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Artikel 8 Absatz 3 erlassen hat, nicht einhalten.

235.1

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020 (Stand am 1. September 2023)

Art. 65 Zuständigkeit

[1] Die Verfolgung und die Beurteilung strafbarer Handlungen obliegen den Kantonen.

[2] Der EDÖB kann bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen.

Art. 66 Verfolgungsverjährung

Die Strafverfolgung verjährt nach fünf Jahren.

The Roadmap to Compliance

Sie müssen das neue Datenschutzrecht ab 1.9.2023 einhalten und als verantwortliche Personendaten-bearbeiter dafür die notwendigen Nachweise erbringen.

Das ist eine gesetzliche Pflicht

KI-spezifische Überlegungen aus datenschutzrechtlicher Sicht

KI-Aspekte aus rein datenschutzrechtlicher Sicht

KI bringt Gefahren: Denn KI-Systeme speichern Daten und verwenden sie weiter. Werden vertrauliche Daten in nicht abgesicherte Tools eingegeben, können sie weitergegeben und weiterverwendet werden. Das verstösst gegen das Datenschutzgesetz und kann zu Reputationsschäden und rechtlichen Konsequenzen führen.

Sofern in KI-Systemen nur **Sachdaten** oder **Informationen ohne Personen-bezug** bearbeitet werden, sind sie grundsätzlich datenschutzrechtlich nicht relevant.

Sobald mit KI Personendaten bearbeitet werden, sind die geltenden Datenschutzvorschriften einzuhalten. Das Datenschutzgesetz (DSG) ist technologieneutral formuliert und auf Innovationen anwendbar.

Zweckbindung als Bremse für KI-Einsatz

Beim Training von KI-Modellen wird oft der Grundsatz der Zweckbindung kompromittiert, da die verwendeten Daten ursprünglich in einem anderen Kontext für einen anderen Zweck erhoben wurden. Eine Zweckänderung muss gerechtfertigt werden; dabei sind insbesondere die Einwilligung der betroffenen Person oder der Rechtfertigungsgrund von Art. 31 Abs. 2 lit. e DSG einschlägig

e. Der Verantwortliche bearbeitet die Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung oder Statistik, wobei die folgenden Voraussetzungen erfüllt sind:

1. Er anonymisiert die Daten, sobald der Bearbeitungszweck dies erlaubt; ist eine Anonymisierung unmöglich oder erfordert sie einen unverhältnismässigen Aufwand, so trifft er angemessene Massnahmen, um die Bestimmbarkeit der betroffenen Person zu verhindern.

2. Handelt es sich um besonders schützenswerte Personendaten, so gibt er diese Dritten so bekannt, dass die betroffene Person nicht bestimmbar ist; ist dies nicht möglich, so muss gewährleistet sein, dass die Dritten die Daten nur zu nicht personenbezogenen Zwecken bearbeiten.

3. Die Ergebnisse werden so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind.

Rechtfertigungsgründe für die Personendatenbearbeitung (nDSG Schweiz)

Art. 31 Rechtfertigungsgründe

1 Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

2 Ein überwiegendes Interesse des Verantwortlichen fällt insbesondere in folgenden Fällen in Betracht:

a. Der Verantwortliche bearbeitet die Personendaten über die Vertragspartnerin oder den Vertragspartner in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags.

Für die **Bearbeitung** von Personendaten **auf einer KI-Plattform**:

- **Einwilligung der betroffenen Person** **(einzig möglicher Rechtfertigungsgrund)**
- Gesetzesgrundlage Keine
- Überwiegendes öffentliches Interesse Keines
- Überwiegendes privates Interesse (ist das „*unmittelbarer Zusammenhang*“?)

Vollständige, irreversible Anonymisierung von Personendaten

Handlungsbedarf 1 für CH-Unternehmen

- Welcher Datenschutzgesetzgebung untersteht ihr Unternehmen? (DSGVO / nDSG)
- Kommt der EU AI Act für Ihr Unternehmen zur Anwendung?
- Ist Ihr Unternehmen auf die Übernahme der Europaratskonvention 2024 vorbereitet? (Ende 2026/2027)

In sichere KI investieren

Unternehmen tun gut daran, betriebliche Leitlinien zu erfassen und ihre Mitarbeitenden für die Gefahren, die bei der Anwendung der KI entstehen können, zu schulen. Für Unternehmen im EU-Raum ist das seit dem 2. Februar 2025 bereits verpflichtend. Eine weitere Möglichkeit ist es, dass Unternehmen in sichere KI-Modelle investieren.

Leitlinien (KI-Weisung) und Schulung -> Nachweispflicht

KI-Aspekte aus rein datenschutzrechtlicher Sicht (11)

KI-Tools: Weisung und Schulung der Mitarbeitenden betreffend KI im Unternehmen

Viele Unternehmen evaluieren zurzeit verschiedene KI-Tools, um diese einzusetzen. Dabei wird der Fokus vermehrt auf die Prüfung des Anbieters gelenkt. Dieser wird aus verschiedenen rechtlichen Perspektiven, wie beispielsweise dem Datenschutzrecht, der Datensicherheit oder dem Urheberrecht, durchleuchtet. An die interne Regelung und Schulung im Umgang mit solchen Tools wird oft erst nachgelagert gedacht. Doch auch intern sollten Unternehmen gewisse Regelungen festhalten und die Mitarbeitenden entsprechend schulen, um die bestehenden Risiken beim Einsatz von KI-Tools auf ein annehmbares Mass zu reduzieren.

https://www.weka.ch/themen/datenschutz-und-it-recht/kuenstliche-intelligenz-und-recht/article/ki-tools-weisung-und-schulung-der-mitarbeitenden-betreffend-ki-im-unternehmen/

Handlungsbedarf 2 für CH-Unternehmen

Das bedeutet in der Praxis:

1. Arbeitnehmende dürfen keine sensiblen oder personenbezogenen Daten in KI-Tools eingeben.
2. Da Unternehmen für die Gesundheit und Sicherheit ihrer Mitarbeitenden sorgen müssen, gehört auch der grundsätzliche Schutz vor Überwachung und Kontrolle durch KI-Tools dazu.
3. Zudem sind Arbeitgeber*innen verpflichtet, ihre Mitarbeitenden zu informieren, falls sie in Ausnahmefällen im erlaubten Rahmen KI zur Analyse oder Überwachung der Arbeit einsetzen und darüber hinaus die Einwilligung der Mitarbeitenden einzuholen, wo dies erforderlich ist.
4. Arbeitnehmende dürfen jederzeit Auskunft von der Arbeitgeber*in verlangen, welche Daten über sie bearbeitet werden und wofür. Es dürfen nur Daten über Arbeitnehmende erhoben und bearbeitet werden, die notwendig sind und nur zum angegebenen Zweck. Die erhobenen Daten sind von der Arbeitgeber*in durch technische und organisatorische Massnahmen zu schützen.

edö-bot 2.0

DE

von David Vasella
am 31.10.2026

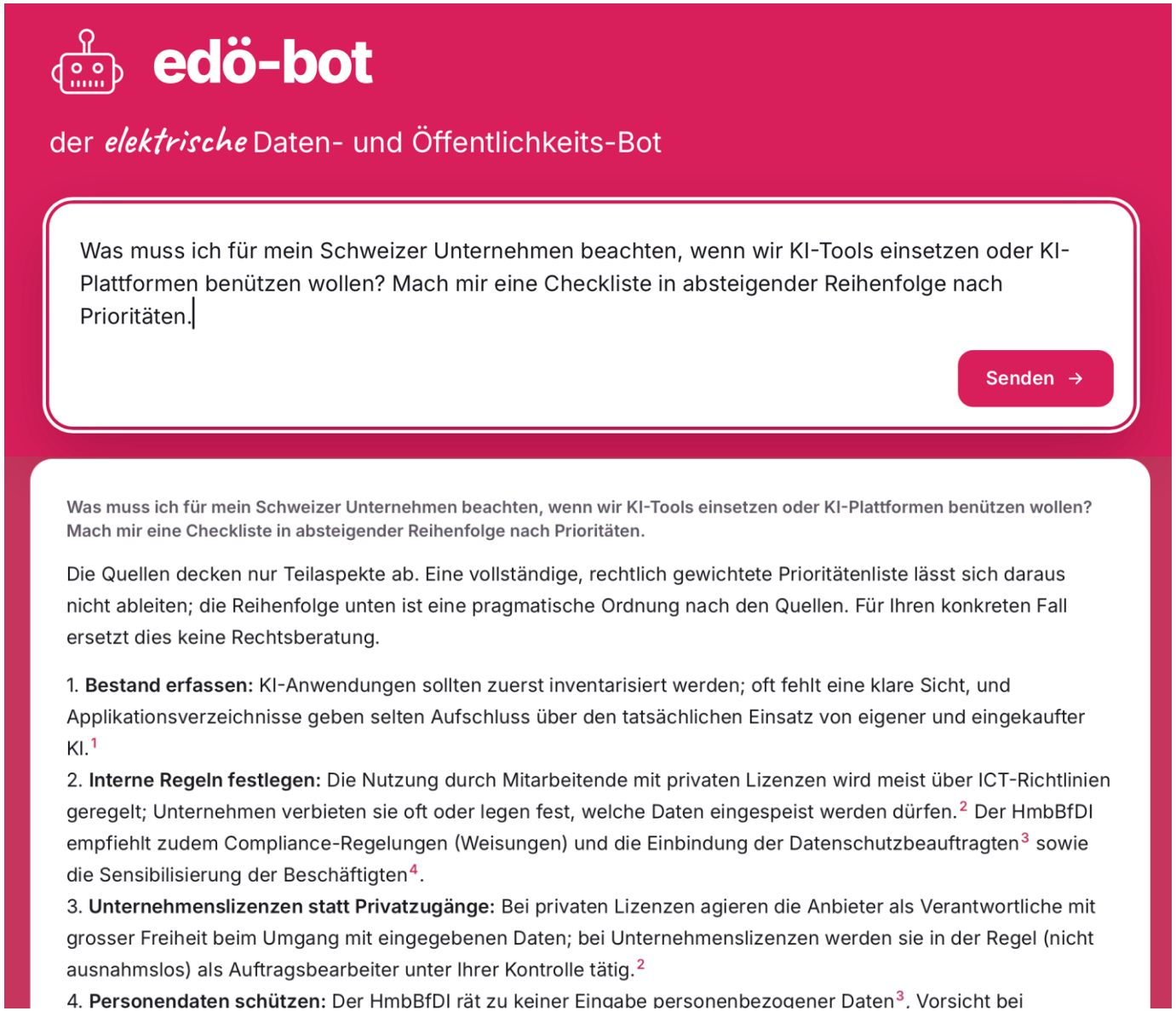
www.edoebot.ch.

Der Bot beantwortet Fragen zum Datenschutz und zum Öffentlichkeitsprinzip der Bundesverwaltung gestützt auf eine Quellensammlung aus rund 740 Dokumenten des EDÖB (Empfehlungen, Schlussberichte, Verfügungen, Leitfäden und die Tätigkeitsberichte seit 1993), die rund 1'450 Beiträge von datenrecht.ch und die einschlägigen Erlasse. Die Antworten geben jeweils die Quellen an und verlinken auf die relevante Fundstelle.

Der edö-bot beruht nicht mehr wie die Vorgängerversion auf einem nicht besonders effektiven Fine-tuning. Er sucht stattdessen zu jeder Frage zunächst die passenden Stellen in den Quellen, mit einer Stichwort- und einer semantischen Suche. Die passenden Passagen und die einschlägigen Gesetzesbestimmungen gehen dann an Claude, der (oder die) die Antworten formuliert und sie mit diesen Quellen belegt.

https://datenrecht.ch/edoe-bot-2-0/?utm_source=datenrecht&utm_campaign=a9ddbaeba3-datenrecht-Mailchimp&utm_medium=email&utm_term=0_15155ce73b-a9ddbaeba3-90792857

AACSB ACCREDITED



www.edoebot.ch.

weblaw

Anonymisierung

Mandantendaten haben in ChatGPT nichts verloren.

Unsere Lösung findet und ersetzt personenbezogene Daten in Ihren Dokumenten, damit Sie jedes KI-Tool nutzen können, ohne personenbezogene Daten preiszugeben.

Läuft komplett auf Ihrem Rechner.

[ORG_1]

[ADDRESS_1] · Tel. [PHONE_1] · [EMAIL_1]

[ORG_1] · [ADDRESS_1]

[ORG_2]

Frau Rechtsanwältin [PERSON_1]

[ADDRESS_2]

München, 30. Juni 2026

Unser Zeichen: [CASE_1] Ihr Zeichen: [CASE_2]

Betreff: Forderung aus Werkvertrag – [PERSON_2] ./. Frau [PERSON_3]; [CASE_3] (Landgericht München I)

Sehr geehrte Frau Kollegin [PERSON_1],

in vorbezeichneter Angelegenheit zeige ich an, dass ich die rechtlichen Interessen von Herrn [PERSON_2], geboren am [DATE_1], wohnhaft [ADDRESS_3], vertrete. Eine entsprechende [ABC_1] liegt anbei.

Ihre Mandantin, Frau [PERSON_3], schuldet meinem Mandanten aus dem Werkvertrag vom 3. Februar 2026 einen restlichen Werklohn in Höhe von 15.480,00 EUR. Trotz Fälligkeit und anwaltlicher Mahnung vom 2. Juni 2026 ist eine Zahlung bislang nicht erfolgt.

weblaw

01 1. Dokument hinzufügen

Text einfügen oder PDF, Word, Excel, CSV, RTF, ODT, E-Mail (.eml/.msg) oder Scan ablegen. Nichts wird hochgeladen. Alles öffnet lokal.

02 2. Erkennungen prüfen

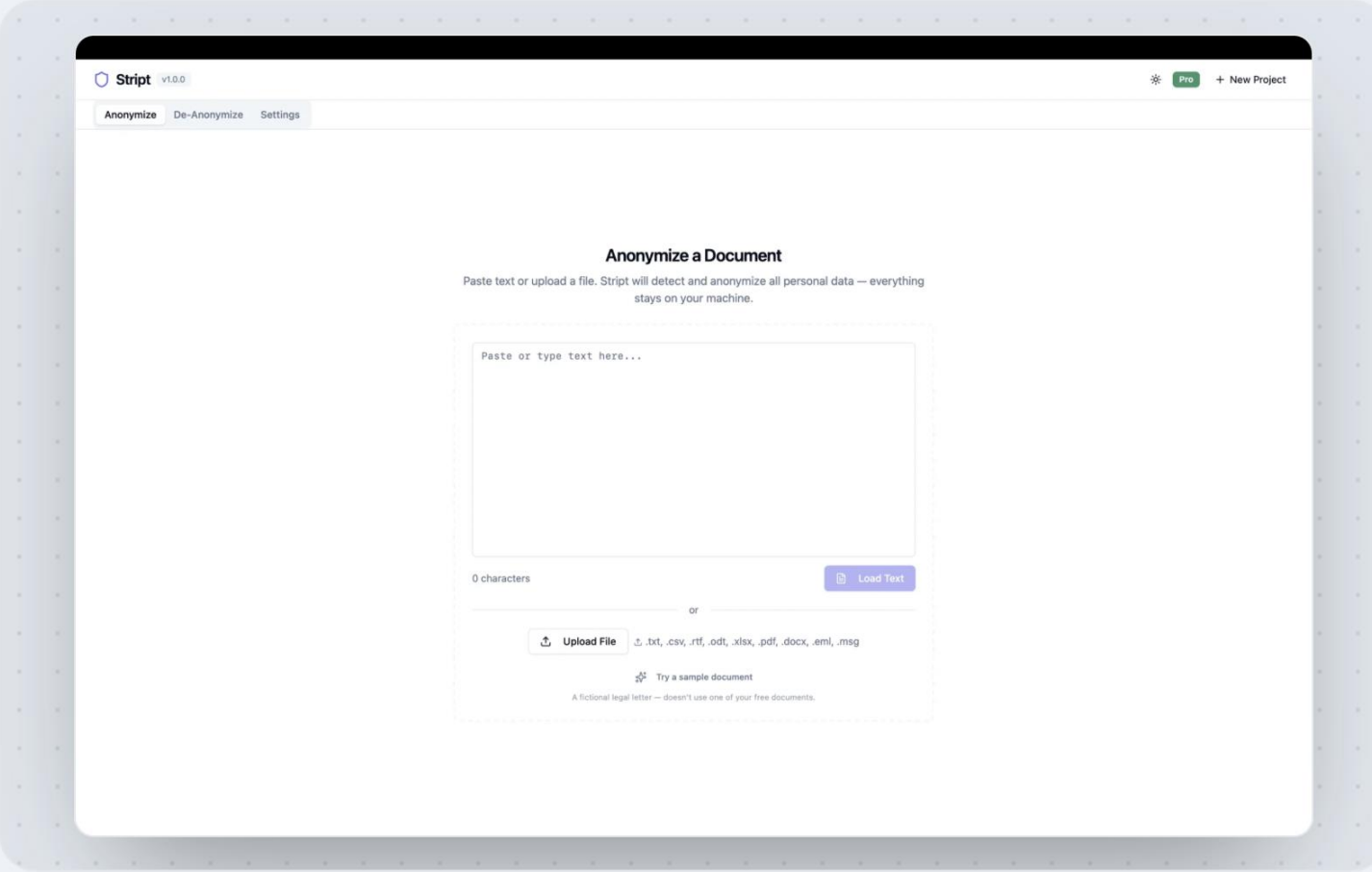
Die Lösung markiert Namen,...

03 3. Anonymisieren und KI nutzen

Konsistente Platzhalter ersetzen die...

04 4. Originale wiederherstellen

Fügen Sie die KI-Antwort zurück ein,...



https://weblaw.ch/produkte/anonymisierung

Konkrete Rechtsfolgen aus der Praxis

Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Abteilung I
A-4467/2025

Urteil vom 13. Oktober 2026

Besetzung

Richterin Christine Ackermann (Vorsitz),
Richter Stephan Metzger,
Richter Alexander Misic,
Gerichtsschreiber Roland Hochreutener.

Parteien

PostFinance AG,
Mingerstrasse 20, 3030 Bern,
vertreten durch lic. iur. David Rosenthal, Rechtsanwalt,und
lic. iur. Adrian Gautschi, Rechtsanwalt,
Vischer AG,
Schützengasse 1, Postfach, 8021 Zürich 1,
Beschwerdeführerin,

gegen

Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter EDÖB,
Feldeggweg 1, 3003 Bern,
Vorinstanz.

Gegenstand

Datenschutz; Authentifizierung mittels Stimmerkennung;
Verfügung vom 16. Mai 2025.

1. Rechtlicher Rahmen & Grundsätze (Stimmerkennung / Sprachaufzeichnungen)

- **Besonders schützenswerte Personendaten:** Das Bundesverwaltungsgericht hat in wegweisenden Urteilen – etwa zur Stimmerkennung bei Finanzinstituten – bestätigt, dass biometrische Stimmabdrücke und Sprachprofile zur eindeutigen Identifikation einer Person zählen und als **besonders schützenswerte Personendaten** im Sinne des Datenschutzgesetzes (DSG) gelten. EDÖB +1
- **Erfordernis einer ausdrücklichen Einwilligung:** Nach der Rechtsprechung des Bundesverwaltungsgerichts reicht es *nicht* aus, wenn Kunden lediglich per Bandansage informiert werden und durch Weitersprechen (oder Nicht-Widersprechen) implizit zustimmen. Eine rechtskonforme Datenbearbeitung setzt eine **ausdrückliche Einwilligung** nach angemessener Information voraus. Stimmprofile, die ohne eine solche gültige Einwilligung erhoben wurden, müssen in der Regel gelöscht oder nachgebessert werden. Bundesverwaltungsger... +1

Fazit:

Verantwortung und Sorgfaltspflichten der Führungskräfte hinsichtlich der Digitalisierung im Unternehmen stellen hohe Anforderungen an die Führungskräfte aller Stufen.

Aufgaben kann man delegieren,
Verantwortung NIE

Compliance- und Risk-Management

- Der Umgang mit allen digitalen Risiken im Unternehmen gehört in den Aufgabenbereich des VR und der GL (Führungsaufgabe: Art. 716 Abs. 5 OR)
- Rasanter technologischer Wandel (z.B. auch KI) zwingt zu periodischer, mindestens einmal jährlicher Überprüfung der veranlassten technischen und organisatorischen, prozessualen und personellen sowie finanziellen Massnahmen zur Vermeidung von digitalen Risiken
- **Die Beweislast für die Erfüllung der Sorgfaltspflichten liegt bei GL und VR**
- Die Haftung dehnt sich in den persönlichen Bereich aller Mitgliedern der GL und VR aus (Grobfahrlässigkeit).

Aufgabe

Standortbestimmung:

Reflektiere (jeder für sich):
wo stehe ich mit meinem Unternehmen bei der Umsetzung der Regularien, die ich im Tag 1 gehört habe?

Erstelle dazu eine Checkliste, welche Punkte in Deinem Unternehmen jetzt zu klären sind.

Danke!



30.10.2026