


# CAS Digitalisierung und Künstliche Intelligenz im HRM

Wissen und innovative Praxis für Gegenwart und Zukunft


Rechtsanwälte
ATTORNEYS @ LAW
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch
Impressum
Datenschutzbestimmungen
Profil
Kompetenzen
Team
Aktuell
Publikationen
Referenzen
Kontakt
Hinweis schliessen
Umsetzung der DSGVO
Als Anwaltskanzlei mit Schwerpunkt vor allem im Datenschutzrecht ist uns ein verantwortungsbewusster Umgang mit Ihren personenbezogenen Daten wichtig. FSDZ Rechtsanwälte & Notariat AG verzichtet vollständig auf den Einsatz von Social Media-Plugins, Websiteanalyse-Diensten und Anzeigen sowie Marketing-Diensten (keine Cookies, keine Google Analytics etc.). Sie können ohne Angabe von personenbezogenen Daten unsere Webseite besuchen.
Jetzt anrufen 041 727 60 80
oder E-Mail schreiben
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
Fax +41 41 727 60 85
sekretariat@fsdz.ch
Karte Google Maps
Rechtsanwalt
lic. iur. Lukas Fässler
Telefon +41 41 727 60 80
Mobile +41 79 209 24 32
faessler@fsdz.ch
Rechtsanwältin und Notarin
lic. iur. Carmen de la Cruz Böhringer
Telefon +41 41 727 60 80
sekretariat@fsdz.ch
Assoziierte selbständige Anwältin:
Eva Patroncini
Büro Uster
Imkerstasse 7
Postfach 1280
CH-8610 Uster
Telefon +41 44 380 85 85
patroncini@fsdz.ch
Partnerkanzlei de la cruz beranek Rechtsanwälte AG, Zug
de la cruz beranek Rechtsanwälte AG
Industriestrasse 7
CH 6300 Zug

www.fsdz.ch

# Lukas Fässler Rechtsanwalt

**Rechtsanwalt und Informatikexperte,**
**Certified Software Asset Manager IAITAM Inc.**

## Profil

| | |
|---|---|
| 1975 – 1980 | Studium an der Universität Fribourg/CH |
| 1982 | Anwaltspatent des Kantons Luzern |
| 1982 – 1984 | Gerichtsschreiber am Amtsgericht Hochdorf |
| 1984 - 1987 | Gerichtsschreiber am Verwaltungsgericht Luzern |
| 1987 - 1992 | EDV-Beauftragter im Gerichtswesen Kanton Luzern |
| 1992 - 1997 | Informatikchef des Kantons Luzern |
| 1997 | Selbständiger Spezialanwalt seit September 1997 |
| 1999 - 2000 | Universität Zürich, Nachdiplomstudium, Internationales Wirtschaftsrecht (Spezialisierungskurs Immaterialgüterrecht, Technologie- und Informationsrecht) |
| 2017 | "Certified Software Asset Manager IAITAM Inc." bei der International Association of Information Techology Asset Managers Inc. in Amerika |

| | |
|---|---|
| VRP AR Informatik AG | (2019) |
| Vizepräsident VR ILZ OW/NW | (2001) |
| Vizepräsident VR HIN AG | (2000) |
| Präsident Verein SSGI | (2005-2025) |
| VRP Viacar AG | (2010-2012) |
| Dozent Fachhochschule NW in Basel | |
| Dozent Universität Basel | |
| Dozent Universität Bern/Lausanne | |

# Zunahme der Risikosituation (1)

# Zunahme der Risikosituation (2)

Cyberangriff auf Comparis

**Comparis-Hacker hatten Zugang zu Nutzerdaten**

Aktualisiert um 08:28 Uhr

https://www.srf.ch/news/wirtschaft/cyberangriff-auf-comparis-comparis-hacker-hatten-zugang-zu-nutzerdaten

Cyberkriminalität

**Emil Frey-Gruppe wurde Opfer von Cyberangriff**

Mittwoch, 12.01.2022, 01:44 Uhr

https://www.srf.ch/news/schweiz/cyberkriminalitaet-emil-frey-gruppe-wurde-opfer-von-cyberangriff

**Hacker legen einzige Zeitungspapierfabrik der Schweiz lahm – Folgen nicht absehbar**

https://www.watson.ch/digital/schweiz/744582672-hacker-legen-einzige-zeitungspapierfabrik-der-schweiz-lahm-mit-folgen

**Hackerangriff auf die Rothenburger Auto AG Group**

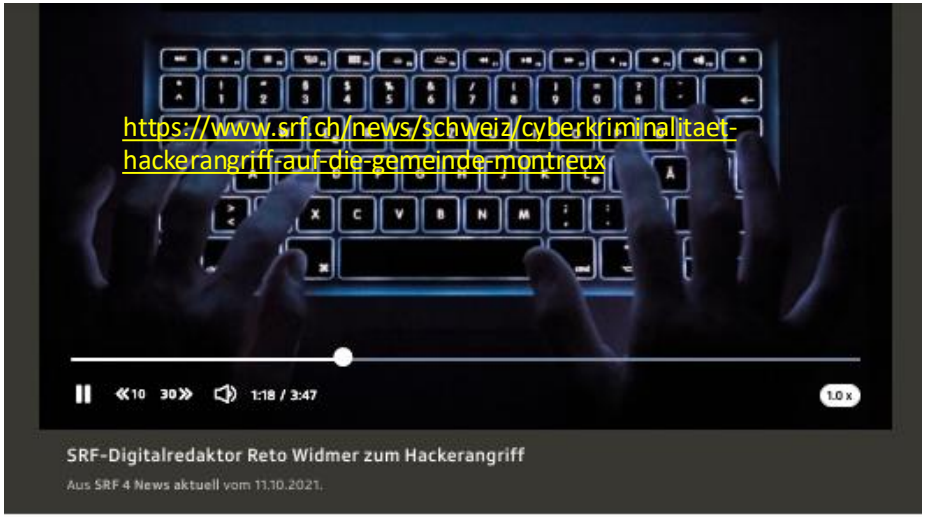
Die Auto AG Group mit Sitz in Rothenburg wurde Opfer eines Hackerangriffs. Die Täterschaft ist bisher unbekannt.

27.08.2019, 17.26 Uhr

Merken Drucken Teilen


Das Gebäude der Auto AG Group in Rothenburg. (Bild: Nadia Schärli, Rothenburg, 16. April 2019)

# Zunahme der Risikosituation (3)




Quelle:
https://www.srf.ch/news/schweiz/cyberkriminalitaet-hackerangriff-auf-die-gemeinde-montreux

News > Schweiz >

Cyberkriminalität

## Hackerangriff auf die Gemeinde Montreux

Montag, 11.10.2021, 08:17 Uhr
Aktualisiert um 11:33 Uhr

Dieser Artikel wurde **4**-mal geteilt.

- Die Waadtländer Gemeinde Montreux ist Ziel eines Cyberangriffs geworden.
- Die Attacke sei am Sonntagmorgen entdeckt worden, teilte die Gemeinde mit. Die Grösse des Angriffs und der Schaden können erst jetzt eingeschätzt werden, teilt die Gemeinde mit.

# Zunahme der Risikosituation (4)

SPAM-MAILS

## Hackerangriff auf Apotheker

APOTHEKE ADHOC, 11.01.2014 09:37 Uhr


Gefälschte E-Mail: Ein Hacker will mit Daten aus dem Postfach eines Apothekers Kasse machen.

Foto: APOTHEKE ADHOC

***Berlin*** **- Nach einem Hackerangriff wurde einem Apotheker aus Niedersachsen nicht nur das Passwort geknackt – ein bislang Unbekannter hat auch im Namen von Dr. Rainer Camehn in einer E-Mail um Geld gebeten. Noch ist der Hackerangriff auf das Postfach des**

# Teil 1

# Digitale Verantwortung im Unternehmen und in öffentlichen Verwaltungen

# Die digitale Verantwortung

- Applikationen und digital unterstützte Prozesse im Unternehmen sind nicht mehr wegzudenken.

- Es besteht eine vollständige Abhängigkeit von der Digitalisierung im Unternehmen.

- Damit stellt die Digitalisierung vollständig neue Anforderungen an die strategischen (Verwaltungsrat) und operativen Führungskräfte (Geschäftsleitung) einer Unternehmung.

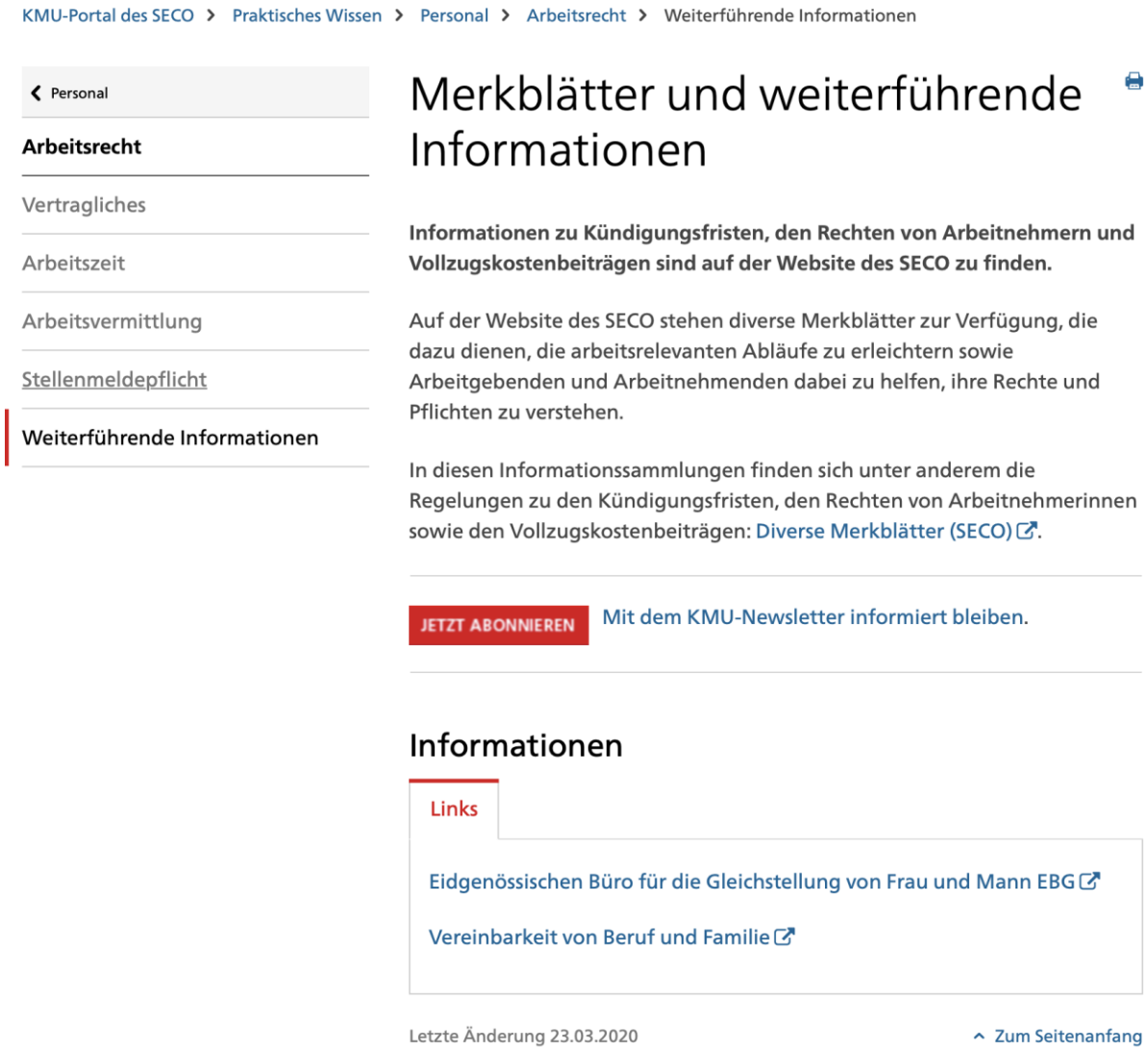
- Die Digitalisierung ist ein zentraler Wirtschaftlichkeitsfaktor, aber zugleich ein erheblicher Risikofaktor im Unternehmen, welche mit aller Sorgfalt zu steuern, überwachen, verbessern sind und die geltenden Bestimmungen (Gesetzes, Verordnungen, Weisungen, Richtlinien, Standards etc.) zu berücksichtigen haben.

# Gesetze und Rahmenbedingungen für die Verantwortung

Im Personalwesen der Schweiz gibt es **kein** einheitliches „**HR-Gesetzbuch**“, sondern ein **Zusammenspiel aus Gesetzen, Verordnungen, branchenspezifischen Regelungen (best practise) und teilweise internationalen Standards**, die HR-Abteilungen beachten müssen. Hier die wichtigsten Bereiche:

## 1. Gesetzliche Grundlagen (obligatorisch)

- **Obligationenrecht (OR)**:
  - Arbeitsvertrag (Art. 319–362 OR)
  - Lohnfortzahlung, Überstunden, Kündigungsschutz, Konkurrenzverbot etc.
- **Arbeitsgesetz (ArG) und Verordnungen**:
  - Arbeits- und Ruhezeiten, Nacht-/Sonntagsarbeit, Gesundheitsschutz
- **Datenschutzgesetz (DSG)** (seit 1.9.2023 revidiert):
  - Schutz von Personaldaten, Informationspflichten, Datensicherheit
- **Gleichstellungsgesetz (GlG)**:
  - Verbot der Diskriminierung von Geschlechtern, Lohnanalysen für grössere Unternehmen
- **Berufsbildungsgesetz (BBG)**:
  - Vorschriften für Lehrverhältnisse
- **Sozialversicherungsrecht**:
  - AHV/IV/EO, ALV, BVG (Pensionskasse), UVG (Unfallversicherung), KTG (Krankentaggeld, wenn abgeschlossen)




https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/personal/arbeitsrecht/weiterfuehrende-informationen.html

# 2. Normen und Standards (freiwillig, aber praxisrelevant)

**ISO-Normen im HR-Kontext**:

- **ISO 30414**: Human Capital Reporting (Kennzahlen für Personalmanagement)
- **ISO 10667**: Assessment Services (Standards für Eignungsdiagnostik und das Auswahlverfahren)
- **ISO 26000**: Leitfaden zur gesellschaftlichen Verantwortung (CSR, auch im HR wichtig)

**Swissdec**: Standard für elektronische Lohnmeldungen an Behörden (z. B. AHV, Suva, Steuerämter)

**Good Practice Guidelines von HR Swiss** (Dachverband Human Resources)

**Leitlinien** des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten **EDÖB** unter https://www.edoeb.admin.ch/de/ki-im-alltag

**3. Branchenspezifische Standards / Gesamtarbeitsverträge (GAV)**

In vielen Branchen gelten **Gesamtarbeitsverträge**, die über die gesetzlichen Mindestbestimmungen hinausgehen (z. B. Bau, Gastronomie, Pflege).
Teils verbindlich erklärt durch den Bundesrat.

**4. Soft-Law & Empfehlungen**

- **Code of best practise for corporate governance** (interne Ethikrichtlinien economiesuisse)
- **Diversity & Inclusion Standards** (z. B. Charta der Vielfalt)
- **OECD-Leitsätze für multinationale Unternehmen**

Nachfolgende Ausführungen zur Aktiengesellschaft gelten sinngemäss auch für die Träger öffentlicher Aufgaben (Verwaltungen).

Hier sind jedoch die jeweiligen Organisations-, Verantwortlichkeits- und Haftungsgesetze des Bundes, der Kantone oder – soweit relevant – der Gemeinden zu beachten.

Öffentliche-rechtliche Aktiengesellschaften, Anstalten oder andere juristische Personen des öffentlichen Rechts unterstehen in der Regel einer Spezialgesetzgebung (z.B. AR: eGov-Gesetz; ILZ OW/NW: Konkordats-Vereinbarung der Kantone OW und NW), wobei jeweils die privatrechtlichen Verantwortlichkeitsbestimmungen zur Anwendung gebracht werden.

# Die gesetzlichen Grundlagen zur Unternehmensführung

# Die digitalen Sorgfaltspflichten der Führungskräfte


**Art. 716*a***[430]

2. Unübertragbare Aufgaben

[1] Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes[431] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

[2] Der Verwaltungsrat kann die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen. Er hat für eine angemessene Berichterstattung an seine Mitglieder zu sorgen.


**B. Der Verwaltungsrat**[414]

5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;

**Compliance-Verantwortung**


## B. Der Verwaltungsrat[414]

### Art. 717[433]

IV. Sorgfalts- und Treuepflicht

[1] Die Mitglieder des Verwaltungsrates sowie Dritte, die mit der Geschäftsführung befasst sind, müssen ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren.

[2] Sie haben die Aktionäre unter gleichen Voraussetzungen gleich zu behandeln.

# Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

vom 30. März 1911 (Stand am 1. Juli 2015)

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

**Art. 754**[488]

[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.

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

## Urteilskopf

139 III 24

4. Auszug aus dem Urteil der I. zivilrechtlichen Abteilung i.S. A. und Mitb. gegen X. AG (Beschwerde in Zivilsachen)
4A_375/2012 vom 20. November 2012

## Regeste a

**Art. 754 OR**; aktienrechtliche Verantwortlichkeit.
Haftung des Verwaltungsrats für die Kosten eines erfolglos geführten Prozesses über die Eintragung von Namenaktien im Aktienbuch der Gesellschaft, in dem erkannt wurde, die Verweigerung der Eintragung sei nicht im Interesse der Gesellschaft erfolgt und habe gegen das Gleichbehandlungsgebot der Aktionäre sowie gegen das Rechtsmissbrauchsverbot verstossen (E. 3).

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

**3.2** Nach **Art. 717 Abs. 1 OR** müssen die Mitglieder des Verwaltungsrats, sowie Dritte, die mit der Geschäftsführung befasst sind, ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren. Die gesetzlich normierte Treuepflicht verlangt, dass die Mitglieder des Verwaltungsrats ihr Verhalten am Gesellschaftsinteresse ausrichten. Für die Sorgfalt, die der Verwaltungsrat bei der Führung der Geschäfte der Gesellschaft aufzuwenden hat, gilt ein objektiver Massstab. Die Verwaltungsräte sind zu aller Sorgfalt verpflichtet und nicht nur zur Vorsicht, die sie in eigenen Geschäften anzuwenden pflegen (**BGE 122 III 195** E. 3a S. 198; **BGE 113 II 52** E. 3a S. 56). Das Verhalten eines Verwaltungsratsmitglieds wird deshalb mit demjenigen verglichen, das billigerweise von einer abstrakt vorgestellten, ordnungsgemäss handelnden Person in einer vergleichbaren Situation erwartet werden kann (PETER BÖCKLI, Schweizer Aktienrecht, 4. Aufl. 2009, § 13 N. 575).

Die Sorgfalt richtet sich nach dem Recht, Wissensstand und den Massstäben im Zeitpunkt der fraglichen Handlung oder Unterlassung. Bei der Beurteilung von Sorgfaltspflichtverletzungen hat mithin eine ex ante Betrachtung stattzufinden (vgl. Urteile 4A_74/2012 vom 18. Juni 2012 E. 5.1; 4A_467/2010 vom 5. Januar 2011 E. 3.3; BERNARD CORBOZ, in: Commentaire romand, Code des obligations, Bd. II, 2008, N. 22 zu **Art. 754 OR**; GERICKE/WALLER, in: Basler Kommentar, Obligationenrecht, Bd. II, 4. Aufl. 2012, N. 31c zu **Art. 754 OR**; WATTER/PELLANDA, in: Basler Kommentar, Obligationenrecht, Bd. II, 4. Aufl. 2012, N. 6 zu **Art. 717 OR**).

# Keine Enthaftung bei Grobfahrlässigkeit

## Grobfahrlässigkeit

Grobfahrlässig handelt, wer grundlegende Vorsichtsgebote nicht beachtet, die eine vernünftige Person in der gleichen Situation befolgt hätte und dadurch andere Personen und auch sich selbst in Gefahr bringt. Zur Grobfahrlässigkeit im Strassenverkehr zählen demnach alle Situationen, bei denen man eine grobe Verletzung der Verkehrsregeln begeht, wie also das Überfahren einer Sicherheitslinie oder dass Missachten eines Stoppsignals.

## Was sind die Folgen von grobfahrlässigem Handeln?

Grobfahrlässigkeit wirkt sich auf die Versicherungsleistung bei einem Schadenfall aus. Eine Versicherung hat so das Recht, einen Teil der entstandenen Kosten von der grobfahrlässig handelnden Person zurückzuverlangen. Das wird auch als Regress oder Rückgriffsrecht bezeichnet. Je nach Schwere der Grobfahrlässigkeit kann dieser Anteil zum Beispiel 20%, 50% oder auch mehr betragen.

Eine Organhaftpflichtversicherung gibt somit keine umfassende Schadensdeckung: Nicht für Vorsatz und grobe Fahrlässigkeit. Wird meist in den AVB ausgeschlossen.

Regress auf Verantwortliche bei Grobfahrlässigkeit in den AVB regelmässig vorgesehen.

# Keine Enthaftung ohne Beweise

Gesetzliche Beweislastumkehr zulasten Führungskräfte (VR und GL)

(Art. 100 OR, Art. 97 ff. OR und Art. 754 OR)

Wer seine laufend aktualisierten Sorgfaltspflichten (Auswahl, Unterrichtung und Überwachung nicht) **nicht** beweisen kann, haftet.

# Standards und Normen


economiesuisse

# Swiss Code of Best Practice

Seit dem 1. Juli 2002 existiert zudem der Swiss Code of Best Practice (oder *"Swiss Code"*) vom Dachverband der Schweizer Wirtschaft (economiesuisse). Dieser listet Verhaltensregeln auf, die für eine vorbildliche Corporate Governance notwendig sind. Die Anwendung des Codes basiert auf Freiwilligkeit. Dieser Swiss Code of Best Practice wurde 2007 um zehn Empfehlungen zur Vergütung von Verwaltungsräten und oberstem Management erweitert.[8]

Neueste Ausgabe:

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

## 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.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

**Bundesamt für Energie BFE**
Digital Innovation Office

**Bericht** vom 28 Juni 2021

# Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung

**Datum:** 28 Juni 2021

**Ort:** Bern

**Auftraggeberin:**

Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

**Auftragnehmer/in:**

Deloitte AG
General-Guisan-Quai 38, CH-8022 Zürich
www.deloitte.com/ch

Achtung: Systemrelevante kritische Infrastrukturen unterliegen zusätzlichen Sorgfaltspflichten

# Fazit

- Die gesamte Digitalisierung mit allen Facetten im Unternehmen ist einer periodischen Risikobeurteilung in vielfacher Hinsicht zu unterziehen:

  - Sicherstellung der **Business Continuity** (Verfügbarkeit)
  - Absicherung der Infrastrukturen, Personendaten, Sachdaten, Objektdaten, Finanzdaten etc. (**Infrastructure and data security**)
  - **Einhaltung von Branchenvorgaben** (z.B. Elektrizitätswirtschaft als kritischer Faktor für die Landesversorgung -> Standards und Vorgaben der Bundesbehörden oder der Branche.
  - Zwingende **Einbindung in** das IKS (**interne Kontrolls**ystem) der Unternehmung
  - Periodische Überprüfung nachweisen (mindestens jährlich einmal)

# Teil 2

# HR und das neue Datenschutz- und Datensicherheitsrechts

# Grundprinzipien des neuen europäischen Datenschutzes (DSGVO)

# Warum kann die DSGVO (EU) für ihr Unternehmen relevant sein?

# Marktortprinzip
# Angebot an Bürger in EU - Aufenthalt in EU - BEOBACHTEN

**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.

## Anknüpfungspunkt 1

Angebot von Waren und Dienstleistungen (Art. 3 Abs. 2 lit.a DSGVO)

## Anknüpfungspunkt 2

Überwachung des Verhaltens von Personen in der EU (Art. 3 Abs. 2 lit.b DSGVO)

# Entstehungsgeschichte

- Datenschutzrecht stammt in EU und CH aus 1995
- Januar 2012: EU-Kommission schlägt Massnahmen vor zur Aktualisierung und Modernisierung der Datenschutz-Richtlinie 95/46/EG und des Rahmenbeschlusses (polizeiliche und justizielle Zusammenarbeit) 2008/977/JI

**Ziel:**

**EU-weit einheitliche, an das digitale Zeitalter angepasste Regeln für alle EU-Staaten, um Rechtssicherheit zu verbessern und Vertrauen von Bürgerinnen und Bürger in den digitalen Binnenmarkt zu stärken.**

**Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG**

- Am 24.4.2016 vom EU-Parlament angenommen.
- **Ist am 25.5.2018 in Kraft getreten**
- Gilt ab diesem Datum für alle Akteure, **die auf dem Gebiet der EU tätig sind**

- EU-Verordnung ist in Gesamtheit verbindlich
- EU-Verordnung ist in jedem EU-Land unmittelbar anwendbar (keine nationalen Gesetz mehr notwendig)

- **Aber zahlreiche Ausnahmetatbestände** (Öffnungsklauseln) **eingeführt** (z.B. Ausdehnung auf juristische Personen möglich -> Österreich / alle anderen Länder: nur Schutz der Personendaten natürlicher Personen)

# VERORDNUNGEN

## Datenschutz-Grundverordnung ab 2018

**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)**

# Verordnungstext mit Erwägungen



http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679

I

*(Gesetzgebungsakte)*

## VERORDNUNGEN

**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)**

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

# Verordnungstext mit Erwägungen (2)

in Erwägung nachstehender Gründe:

(1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

(3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (4) ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

# Verordnungstext mit Erwägungen (3)

(172) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 7. März 2012 ([1]) eine Stellungnahme abgegeben.

(173) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([2]) bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten —

([1]) ABl. C 192 vom 30.6.2012, S. 7.
([2]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

# Verordnungstext mit Erwägungen (4)



HABEN FOLGENDE VERORDNUNG ERLASSEN:

*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 2*

**Sachlicher Anwendungsbereich**

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

*Artikel 98*

**Überprüfung anderer Rechtsakte der Union zum Datenschutz**

Die Kommission legt gegebenenfalls Gesetzgebungsvorschläge zur Änderung anderer Rechtsakte der Union zum Schutz personenbezogener Daten vor, damit ein einheitlicher und kohärenter Schutz natürlicher Personen bei der Verarbeitung sichergestellt wird. Dies betrifft insbesondere die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung solcher Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Verkehr solcher Daten.

*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.

# Tracking – Cookies etc.

Die meisten Internetseiten setzen heute standardmässig Analysetools jeder Ausprägung ein (z.B. Google-Analytics, Google Fonts etc.).

**Das ist BEOBACHTEN von BETROFFENEN**

Ist-Zustand

| Land | Unternehmen | Produkt und Verbindungs-URL |
|---|---|---|
| US | Cloudflare, Inc. | CDNJS<br>https://cdnjs.cloudflare.com/ajax/libs/fancybox/3.5.7/jquery.fancybox.min.css |
| US | Cloudflare, Inc. | Cloudflare CDN<br>https://unpkg.com/aos@2.3.1/dist/aos.css |
| US | Google Ireland Limited | Google Analytics<br>https://region1.google-analytics.com/g/collect?v=2&tid=G-5B9CD73C8R&gtm=2oe9q0&_p=1504670904&cid=1855430335.1664458288&ul=en-us&sr=800x600&uaa=&uab=&uafvl=&uamb=0&uam=&uap=&uapv=&uaw=0&_z=ccd.v9B&_s=2&sid=1664458287&sct=1&seg=1&dl=https%3A%2F%2Fwww.fairway-asset.com%2Fweekly-thoughts%2Ffly-me-to-the-moon&dt=Fly%20Me%20to%20the%20Moon%20-%20Weekly%20Thoughts%20-%20Fairway%20Asset%20Management&en=user_engagement&_et=23019 |
| US | Google Ireland Limited | Google CDN<br>https://www.gstatic.com/recaptcha/releases/ovmhLiigaw4D9ujHYlHcKKhP/recaptcha_en.js |
| US | Google Ireland Limited | Google Fonts<br>https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2 |
| US | Google Ireland Limited | Google Tag Manager<br>https://www.googletagmanager.com/gtag/js?id=G-5B9CD73C8R&l=dataLayer&cx=c |
| US | Google Ireland Limited | Google reCAPTCHA<br>https://www.google.com/recaptcha/api.js?render=6Lchoz4aAAAAAGMSgmz8yhJQRuCXnOKJ6I-k1Ilt |
| US | jQuery | jQuery CDN<br>https://code.jquery.com/ui/1.12.1/jquery-ui.min.js |

# Handlungsbedarf für Webseiten

- **Analysetools abschalten**

- **Neue Datenschutzbestimmungen (DSB) verfassen,**
  - **Transparenz- und Koppelungsverbot sicherstellen,**
  - **Widerruf einbinden und**
  - **AUSDRÜCKLICHES EINVERSTÄNDNIS via clickwrapping (z.T. schon auf der Eintrittsseite) abholen und speichern.**

# Schweizerisches Datenschutzgesetz (nDSG)

Bundesdatenschutzgesetz nDSG

- Bundesbehörden
- Private Unternehmen
- Bundesbeauftragte UN

26 kantonale Datenschutzgesetze

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

# Umsetzung in der CH

235.1

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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

- **Vernehmlassung zum Gesetzesentwurf lief bis 4. April 2017**
- **Botschaft des Bundesrates an das Parlament am 15.9.2017**
- **Behandlung im Nationalrat und Ständerat: Beginn 12.6.2018 NR**

- **Parlament hat nDSG am 25.9.2020 verabschiedet**

- **Bundesrat hat die Verordnung zum neuen Datenschutzgesetz am 23.6.2021 in Vernehmlassung geschickt. Wurde in der Zwischenzeit überarbeitet und publiziert.**

- **Der Bundesrat hat Datenschutzgesetz, Verordnung zum Datenschutzgesetz und eine Zertifizierungs-Verordnung am 31.8.2022 in Kraft gesetzt auf den 1.9.2023**
- **https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90134.html**

**Bundesverfassung**
**der Schweizerischen Eidgenossenschaft**

**101**

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.

# Schweizerisches Zivilgesetzbuch

vom 10. Dezember 1907 (Stand am 1. Juli 2013)

II. Gegen Verletzungen
1. Grundsatz

**Art. 28**[30]

[1] Wer in seiner Persönlichkeit widerrechtlich verletzt wird, kann zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen.

[2] Eine Verletzung ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

Zivilrechtliches Klageverfahren vor Bezirks-, Kantons- und Bundesgericht nach ZGB

# Personendaten

# 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:

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;

# Neu: Profiling-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:

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;

# Bearbeitung

# 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;

# Verantwortlicher

**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.

# Aus- und Weiterbildung der Arbeitnehmenden

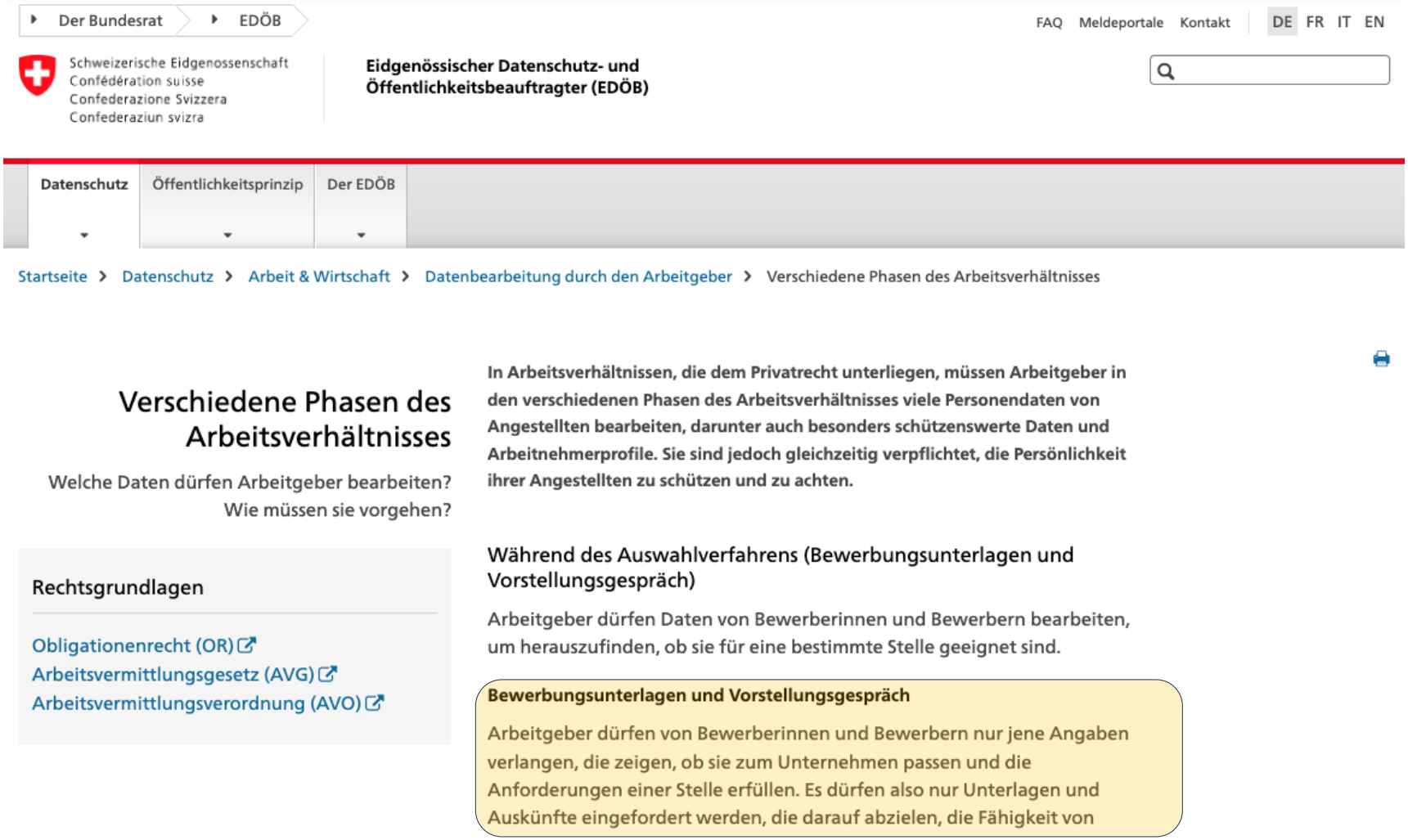
**Art. 10** Datenschutzberaterin oder -berater

[1] Private Verantwortliche können eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

[2] Die Datenschutzberaterin oder der Datenschutzberater ist Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind. Sie oder er hat namentlich folgende Aufgaben:

a. Schulung und Beratung des privaten Verantwortlichen in Fragen des Datenschutzes;

b. Mitwirkung bei der Anwendung der Datenschutzvorschriften.




https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber/datenbearbeitung_arbeitgeber_phasen.html

# Auftragsbearbeiter

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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

**Art. 5** Begriffe

In diesem Gesetz bedeuten:

k. *Auftragsbearbeiter:* private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

# Auslagerung der Datenbearbeitung (inkl. Cloud-Computing)

**Art. 9** Bearbeitung durch Auftragsbearbeiter

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

[4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

# Auftragsdatenverarbeitungsvertrag ADVV

**Art. 28 (1) DSGVO / 9 nDSG**
**Zusammenarbeit mit Auftragsverarbeiter**

Erfolgt eine **Verarbeitung im Auftrag eines** **Verantwortlichen**,

so arbeitet dieser **nur mit** **Auftragsverarbeitern** zusammen,

- die **hinreichend Garantien** dafür bieten,
- dass **geeignete technische und organisatorische Massnahmen** so durchgeführt werden,
- dass die **Verarbeitung im Einklang mit den Bestimmungen der DSGVO** erfolgt und
- der **Schutz der Rechte der Betroffenen gewährleistet** ist.

**Alle Verträge mit Auftragsverarbeitern müssen überprüft und allenfalls angepasst werden.**

**Wer personenbezogene Daten an beigezogene Service-Provider auslagert, muss einen Auftragsdatenverarbeitungsvertrag (ADVV) mit einem Service Level Agreement für TOM's (technische und organisatorische Massnahmen – SLA TOM) abschliessen und vorweisen können.**

# Auftragsdatenverarbeitungsvertrag ADVV

## Art. 28 (2 und 3a-h) DSGVO / 9 nDSG
## Zusammenarbeit mit Auftragsverarbeiter – VERTRAG nötig

**Verantwortlicher** braucht (neue) **Verträge** (ausdrücklich in Art. 28 Abs. 3 DSGVO) mit **Auftragsverarbeiter**, welche

- im Detail die aus der Datenschutz-Folgeabschätzung abgeleiteten organisatorischen oder technischen Massnahmen vertraglich überbinden,
- Selber notwendige und aktuelle Massnahmen sicherstellt,
- Gegenstand und Dauer der Verarbeitung regelt (3),
- Art und Zweck der Verarbeitung regelt (3),
- Nur auf dokumentierte Weisung verarbeitet (3a),
- Bearbeitende Personen zur Vertraulichkeit verpflichtet werden (3b),
- Art der personenbezogenen Daten festlegt (3),
- Kategorien betroffener Personen festlegt (3),
- die Rechte und Pflichten des Auftragsverarbeiters dafür statuiert,
- die Service Levels für die Massnahmen definiert,
- die Gewährleistung des Auftragsverarbeiters festlegt,
- die Informationspflichten bei Verletzungen regelt,
- die Haftung des Auftragsverarbeiters definiert,
- ein jederzeitiges Auditrecht (Kontrollrecht bez. Einhaltung der vertraglichen Auflagen) sicherstellt.

# Ausdrückliche Einwilligung

# Zulässigkeit der Bearbeitung von Personendaten

**Informationspflicht**

**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.

- **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

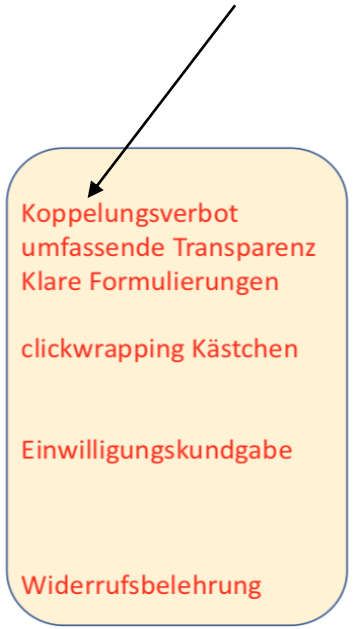
c. ein Profiling durch ein Bundesorgan.

# Ausdrückliche Einwilligung

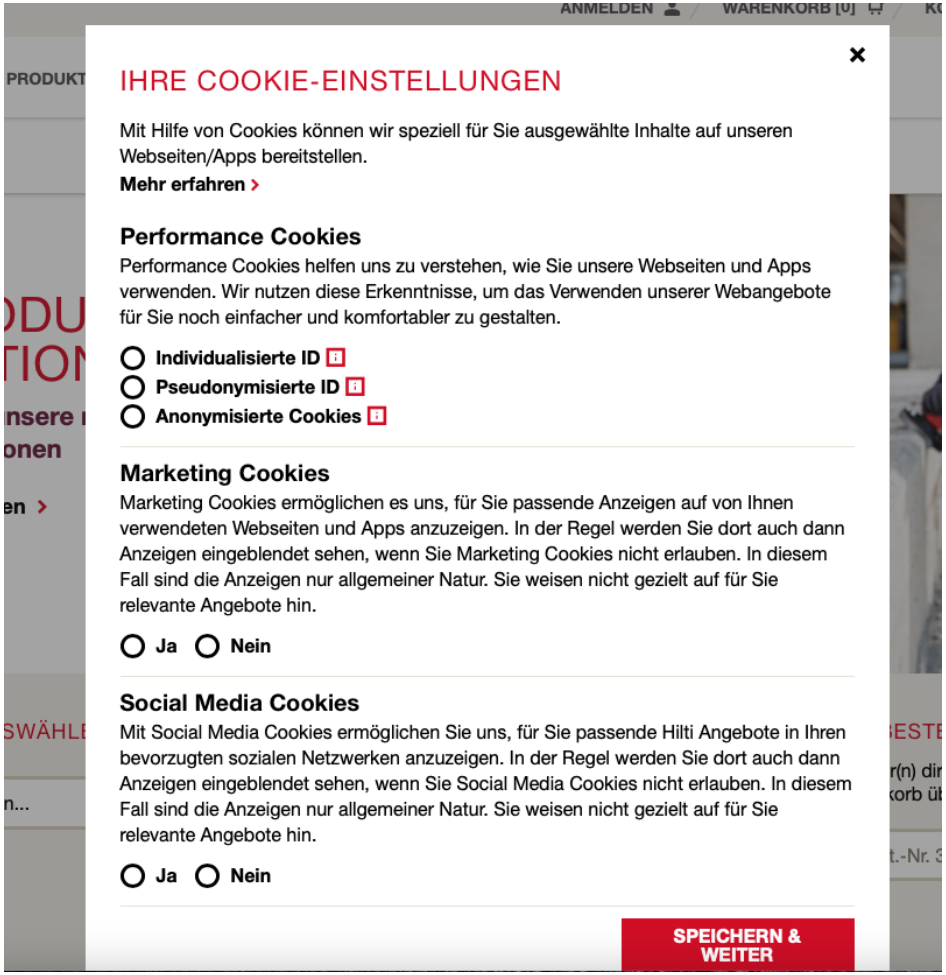
## Art. 4 § 11 DSGVO / Art. 6 Abs. 6 nDSG

- **Ausdrückliche Einwilligung** ist

- jede **freiwillig** für den bestimmten Fall,
- in **informierter** Weise und
- **unmissverständlich** abgegebene Willensbekundung
- in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden **Handlung**,
- mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten **einverstanden** ist.
- Die ausdrückliche Einwilligung ist **jederzeit widerrufbar** (Betroffenenrechte –> eingeschränkte Nutzung –> Anspruch auf Löschung meiner gespeicherten und verarbeiteten personenbezogenen Daten).




Kostenlose Standardlieferung bei Bestellungen ab 100 € und ur
HILTI
PRODUKTE / SERVICES / ENGINEERING / BRANCHEN / UNTERNEHMEN / KARRIERE
Wir sind für Sie da! Unsere Hilti Stores sind bundesweit für Sie geöffnet Mehr ›
NEUPRODUKTE & INNOVATIONEN
Entdecken Sie unsere neuesten Hilti Produktinnovationen
Zu den Neuprodukten ›
PROFITIEREN SIE VON PERSONALISIERTEN WEBANGEBOTEN - DURCH DEN GEZIELTEN EINSATZ VON COOKIES
Mit Ihrer Erlaubnis nutzt Hilti Cookies, um die Verwendung unsere Webseiten/Apps einfacher und komfortabler für Sie zu machen.
COOKIE-EINSTELLUNGEN ANNEHMEN
WÄHLEN SIE IHRE INDIVIDUELLEN COOKIE-EINSTELLUNGEN


ANMELDEN
WARENKORB [0]
PRODUKT
IHRE COOKIE-EINSTELLUNGEN
Mit Hilfe von Cookies können wir speziell für Sie ausgewählte Inhalte auf unseren Webseiten/Apps bereitstellen.
Mehr erfahren ›
Performance Cookies
Performance Cookies helfen uns zu verstehen, wie Sie unsere Webseiten und Apps verwenden. Wir nutzen diese Erkenntnisse, um das Verwenden unserer Webangebote für Sie noch einfacher und komfortabler zu gestalten.
Individualisierte ID
Pseudonymisierte ID
Anonymisierte Cookies
Marketing Cookies
Marketing Cookies ermöglichen es uns, für Sie passende Anzeigen auf von Ihnen verwendeten Webseiten und Apps anzuzeigen. In der Regel werden Sie dort auch dann Anzeigen eingeblendet sehen, wenn Sie Marketing Cookies nicht erlauben. In diesem Fall sind die Anzeigen nur allgemeiner Natur. Sie weisen nicht gezielt auf für Sie relevante Angebote hin.
Ja
Nein
Social Media Cookies
Mit Social Media Cookies ermöglichen Sie uns, für Sie passende Hilti Angebote in Ihren bevorzugten sozialen Netzwerken anzuzeigen. In der Regel werden Sie dort auch dann Anzeigen eingeblendet sehen, wenn Sie Social Media Cookies nicht erlauben. In diesem Fall sind die Anzeigen nur allgemeiner Natur. Sie weisen nicht gezielt auf für Sie relevante Angebote hin.
Ja
Nein
SPEICHERN & WEITER

# EuGH-Urteil vom 1.10.2019 – Az. C-673/17 (2)

Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

Impressum Datenschutzbestimmungen

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

« Zurück zur Übersicht

## Voreingestellte Einwilligung in Cookies ist unzulässig

Verfasst am 01.10.2019

**Der EuGH hat mit einem Urteil entschieden, dass die voreingestellte Einwilligung in Cookies unzulässig ist. Die Internetnutzer müssen demzufolge beim Besuch von Webseiten dem Setzen der Cookies aktiv zustimmen.**

Weiterlesen

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
Fax +41 41 727 60 85
sekretariat@fsdz.ch
Karte Google Maps

# Informationspflichten

**Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)**

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

## 3. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters

**Art. 19** Informationspflicht bei der Beschaffung von Personendaten

[1] Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

[2] Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

a. die Identität und die Kontaktdaten des Verantwortlichen;

b. den Bearbeitungszweck;

c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

Anpassung aller Datenschutzbestimmungen auf Webseiten erforderlich

# Informationspflichten bei automatisierten Entscheidungen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2020
www.bundesrecht.admin.ch
Massgebend ist die signierte elektronische Fassung

*Ablauf der Referendumsfrist: 14. Januar 2021*

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

vom 25. September 2020

## Art. 21 Informationspflicht bei einer automatisierten Einzelentscheidung

1 Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (automatisierte Einzelentscheidung).

2 Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.

3 Die Absätze 1 und 2 gelten nicht, wenn:

a. die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder

b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

# Bearbeitungsverzeichnis

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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

## Art. 12 Verzeichnis der Bearbeitungstätigkeiten

[1] Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.

[2] Das Verzeichnis des Verantwortlichen enthält mindestens:

a. die Identität des Verantwortlichen;

b. den Bearbeitungszweck;

c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;

d. die Kategorien der Empfängerinnen und Empfänger;

e. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;

f. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8;

g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2020
www.bundesrecht.admin.ch
Massgebend ist die signierte elektronische Fassung

*Ablauf der Referendumsfrist: 14. Januar 2021*

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

vom 25. September 2020

## Art. 12 Abs. 5 nDSG

5 Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.

Im Bereich HRM dürfte diese Ausnahmebestimmung NIE zum Tragen kommen. Also braucht es im Unternehmen diesbezüglich (Mitarbeiterdaten) immer ein **Bearbeitungsverzeichnis.**

# Datenschutz-Folgenabschätzung (DSFA) nach n-DSG

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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

**Art. 22** Datenschutz-Folgenabschätzung

1 Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

2 Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;

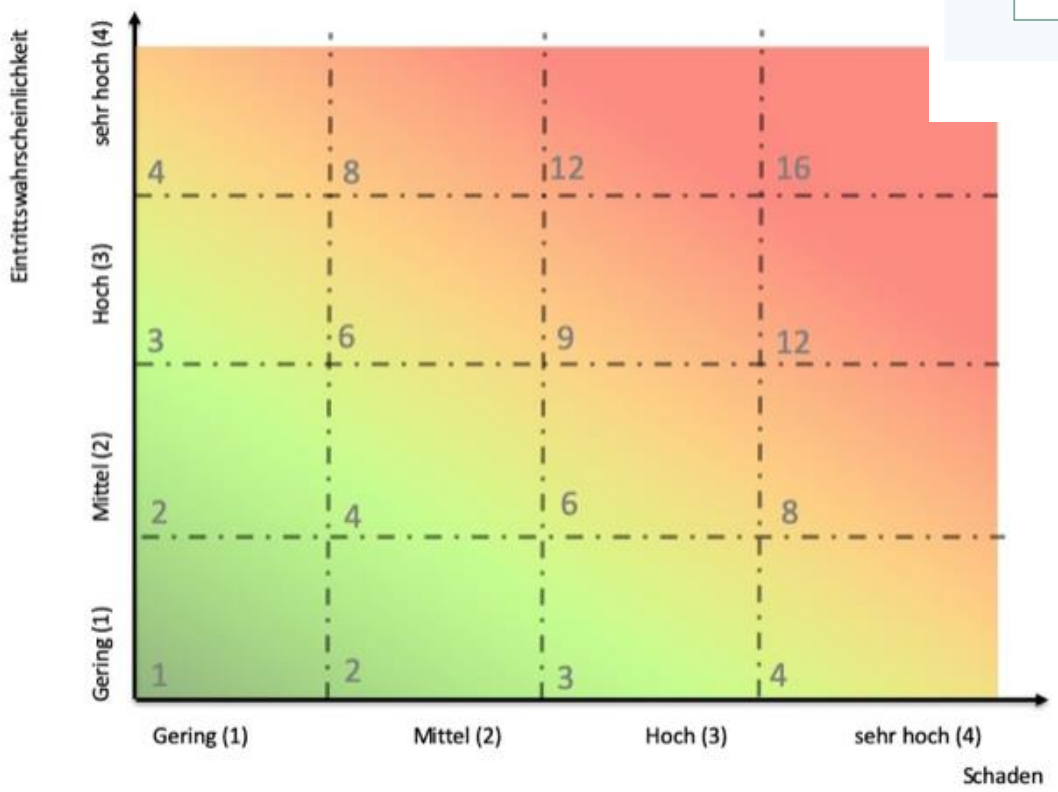
b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

3 Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

# Datenschutz-Folgenabschätzung nach nDSG-CH

## Beispiel

### Risikomatrix




NORM [AKTUELL]

**ISO/IEC 27005:2018-07**

**Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement**

**Englischer Titel:**
Information technology - Security techniques - Information security risk management

**Ausgabedatum:**
2018-07

**Originalsprachen:**
Englisch

# Meldepflichten
## Data Breach Notifications (nDSG)

# Meldung und Benachrichtigung nach nDSG

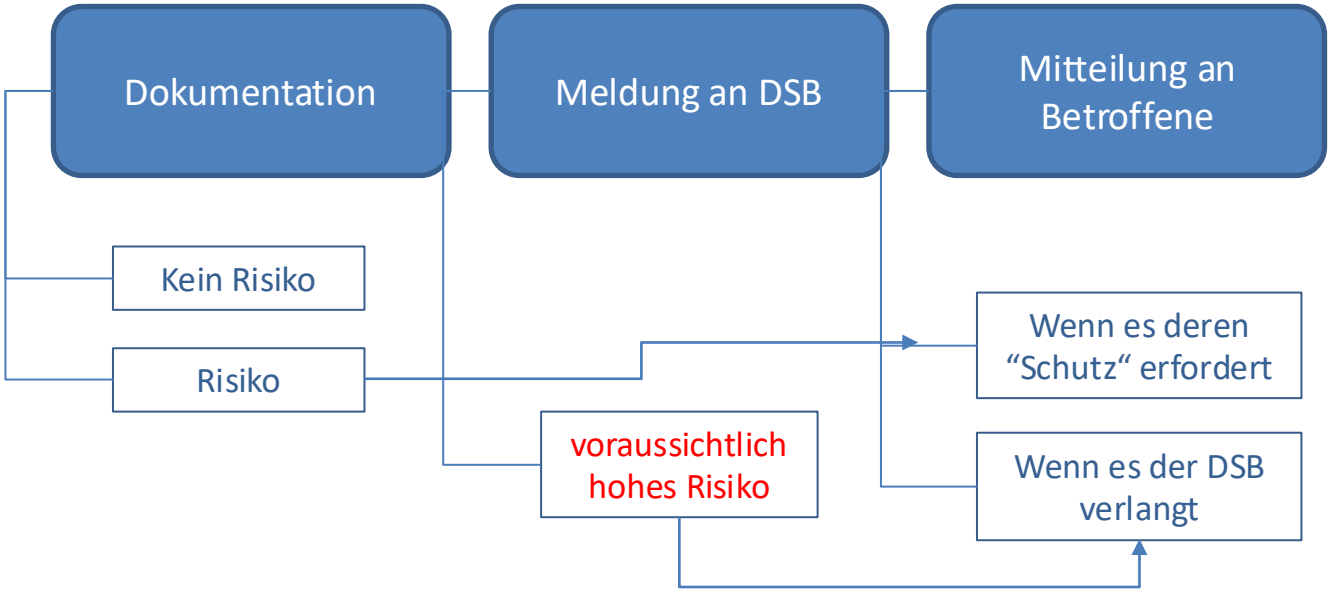
**Art. 24 Meldung von Verletzungen der Datensicherheit**

1 Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

3 Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

4 Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

# Meldung und Benachrichtigung nach nDSG



# Sanktionen der DSGVO

# 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.

# IRLAND: Busse von € 345 Mio. gegen TikTok - Verletzung der Informationspflicht und unzureichende TOMs betr. Kinder

Verfasst am 18.09.2023

**Die Irischen Datenschutzbehörde hat am 1.9.2023 – nach Konsultation verschiedener weiter involvierten Datenschutzbehörden anderer Länder – und nach Einschaltung und Entscheid der EDSA nach Artikel 65 Abs. 1 lit. a DSGVO – gegenüber TikTok eine Busse von EUR 345 Mio verhängt. Es lagen folgende Verstösse gegen die DSGVO vor:**

- **Inhalte waren auch für Kinder standardmässig auf "öffentlich" gesetzt**
- **Mit einer sog. "Familienverknüpfung" konnten Dritte – bspw. Eltern – ihr Konto mit jenem des Kindes verbinden.**
- **Das Risiko, dass Kinder unter 13 dennoch Zugang zur Plattform erhielten, war nie strukturiert eingeschätzt worden. Eine Datenschutz-Folgenabschätzung lag zwar vor, aber dieses Risiko war ausser Acht gelassen worden.**
- **TikTok hatte die Informationspflicht verletzt. Dass bei einer «öffentlichen Kontoeinstellung» Dritte, die nicht TikTok-Benutzer waren, Inhalte einsehen konnten, wurde nicht mitgeteilt.**

# Auch CH-Unternehmen betroffen

Informationspflichten aufmerksam wurde und Beschwerde einreichte. Aufgrund der Beschwerde verpflichtete die österreichische Datenschutzbehörde das Schweizer Unternehmen zur nachträglichen Information des Beschwerdeführers und zur Vervollständigung der Information in Ihrer Datenschutzerklärung innert vier Wochen.

## Schweizer Hotelbuchungsplattform verletzt die DSGVO-Informationspflicht in Österreich

DIENSTAG, 26. NOVEMBER 2019

**Die österreichische Datenschutzbehörde verpflichtet in ihrem Entscheid eine Online-Hotelbuchungsplattform mit Sitz in der Schweiz zur Einhaltung der DSGVO-Informationspflicht. Das Schweizer Unternehmen war den Informationspflichten nur unvollständig nachgekommen und hatte es zudem unterlassen, einen Unionsvertreter zu benennen. Die Anwendbarkeit der DSGVO**

# Sanktionen nach DSGVO

ARTIKEL-29-DATENSCHUTZGRUPPE

17/DE

WP 253

**Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679**

**angenommen am 3. Oktober 2017**

https://www.datenschutzkonferenz-online.de/media/wp/20171003_wp253.pdf

# Sanktionen im Schweizerischen Bundes-Datenschutzgesetz

## (inkl. kantonale DSG)

**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.

**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.

# Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

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

**Art. 62** Verletzung der beruflichen Schweigepflicht

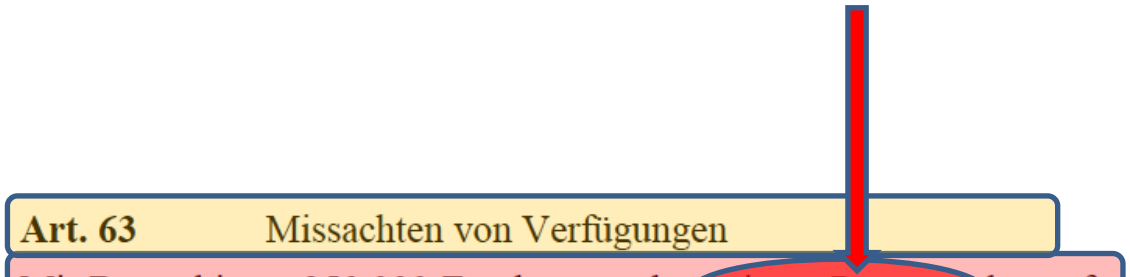
[1] Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.

[2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser Kenntnis erlangt hat.

[3] Das Offenbaren geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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



**Art. 63** Missachten von Verfügungen

Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die einer Verfügung des EDOB oder einem Entscheid der Rechtsmittelinstanzen, die oder der unter Hinweis auf die Strafdrohung dieses Artikels ergangen ist, vorsätzlich nicht Folge leisten.

**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.

# Grundsätze der IT-Sicherheit im neuen Datenschutzrecht

**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:

h. *Verletzung der Datensicherheit:* eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;

**Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)**

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

---

**Art. 7** Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1 Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

2 Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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

---

**Art. 8** Datensicherheit

1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

2 Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Datenbearbeitungsvertrag mit Auftragsbearbeiter (ADVV)

Interne Weisungen und Leitlinien zu KI-Einsatz im Unternehmen
(Vermeidung von Schatten-KI)

**Bundesgesetz**
**über den Datenschutz**
**(Datenschutzgesetz, DSG)**

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

Vertrags- und Auditpflichten für Verantwortlichen

**Art. 9** Bearbeitung durch Auftragsbearbeiter

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

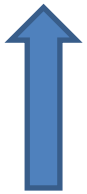

https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

# Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes

August 2015



Wird auf den 1.9.2023 überarbeitet werden

## Inhaltsverzeichnis

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

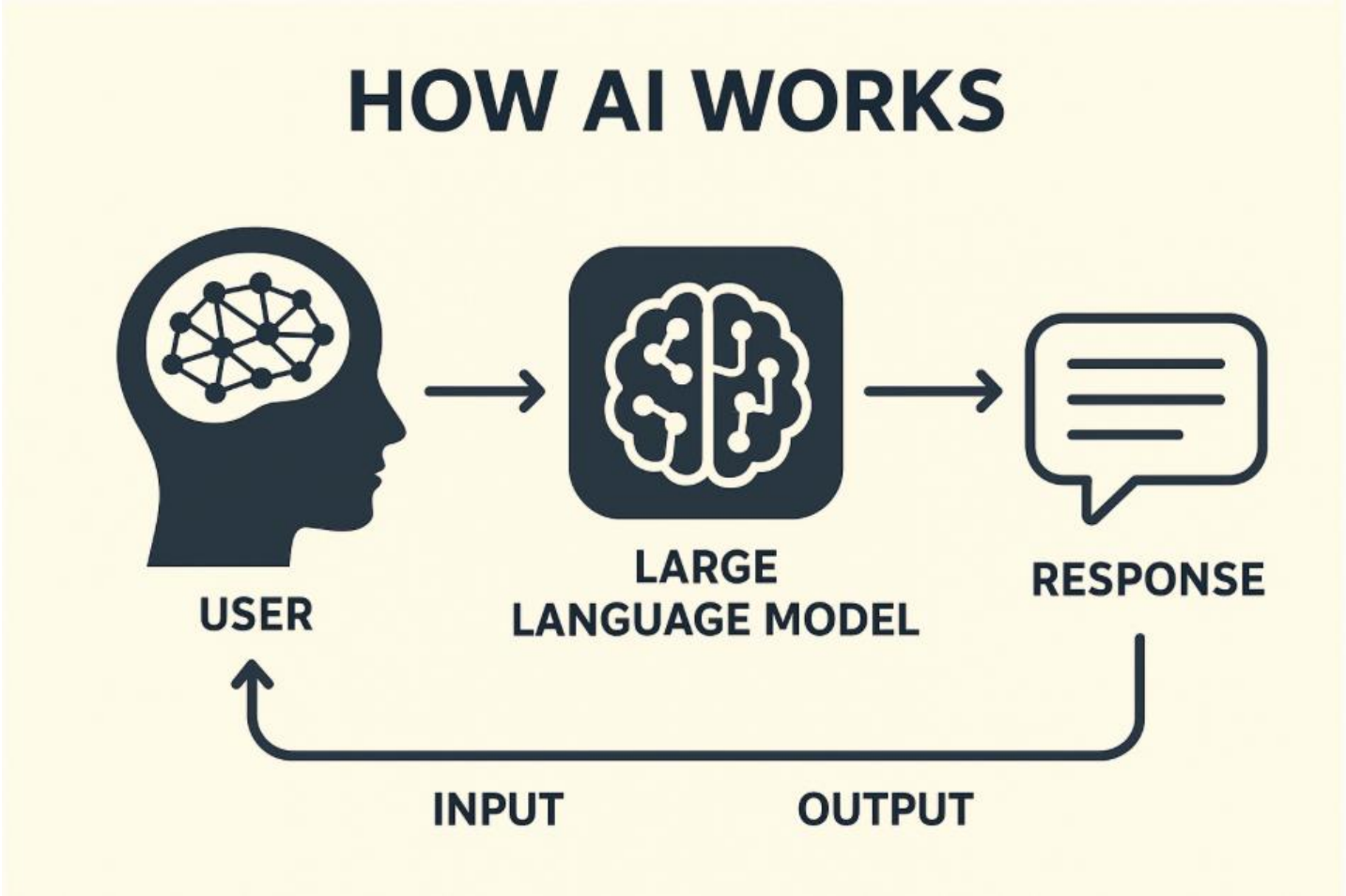
# Künstliche Intelligenz im HR

# Mögliche Einsatzbereiche von KI im Personalwesen

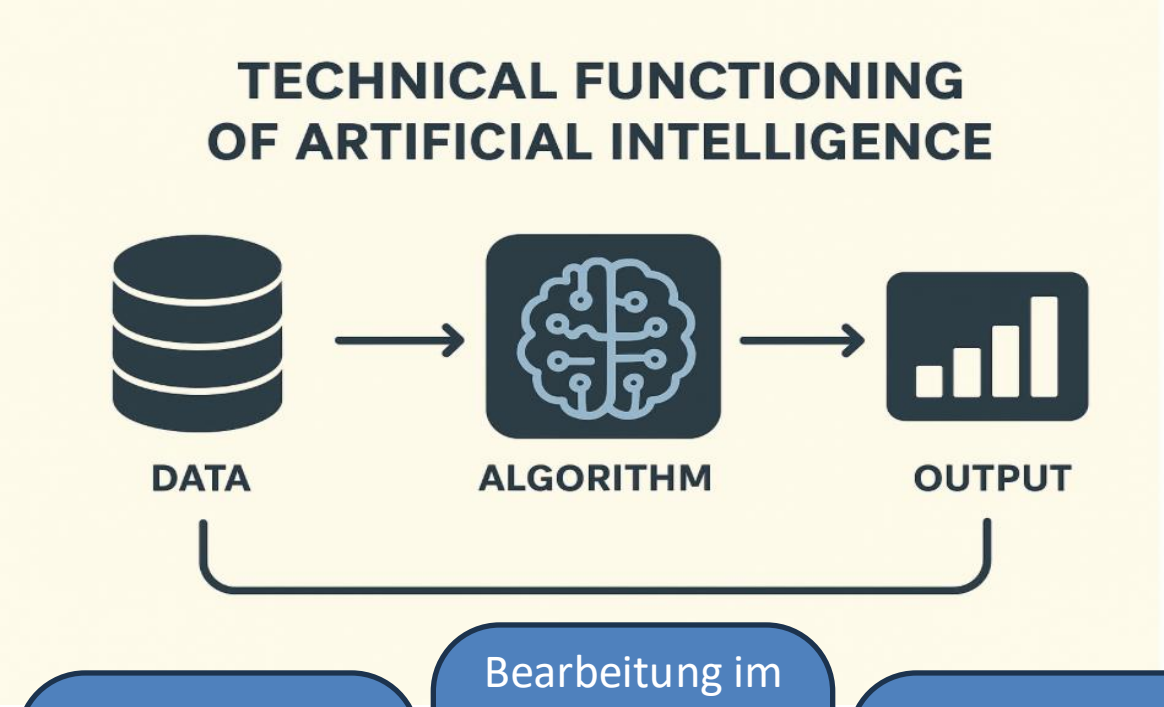
- **Recruiting / Sourcing**: Active Sourcing, Kandidatenrecherche, CV-Matching, Screening, Rankingen von Bewerbern. workday.com +1
- **Kandidaten-Kommunikation & Automatisierung**: Chatbots für Fragen, Interview-Scheduling, Status-Updates. (Rund-um-die-Uhr-Antworten, weniger manueller Aufwand). inside-it.ch
- **Assessment & Video-Interviews**: Automatisierte Auswertung von Tests, Sprach-/Verhaltenssignalen (mit Vorsicht wegen Bias). HR Today
- **Onboarding & L&D**: Personalisiertes Learning, Lernpfade, Skill-Gap-Analysen, Microlearning-Empfehlungen. workday.com
- **HR-Analytics & Workforce Planning**: Fluktuations-/Retention-Vorhersagen, Kapazitätsplanung, Skills-Inventar. workday.com
- **Administrative Automatisierung**: Automatische Vertragserstellung, Dokumentenmanagement, Payroll-Vorbereitung. workday.com
- **Employee Experience / Sentiment**: Analyse von Umfragen, Chat-Logs, Identifikation von Frühwarnsignalen (Engagement, Konflikte). workday.com

Quelle: ChatGPT-Abfrage vom 14.09.2025

# KI-Aspekte aus rein datenschutzrechtlicher Sicht



# KI-Aspekte aus rein datenschutzrechtlicher Sicht (2)




**Informationen**

Textdateien
Bilddateien
Audiodateien
Videodateien
.....dateien

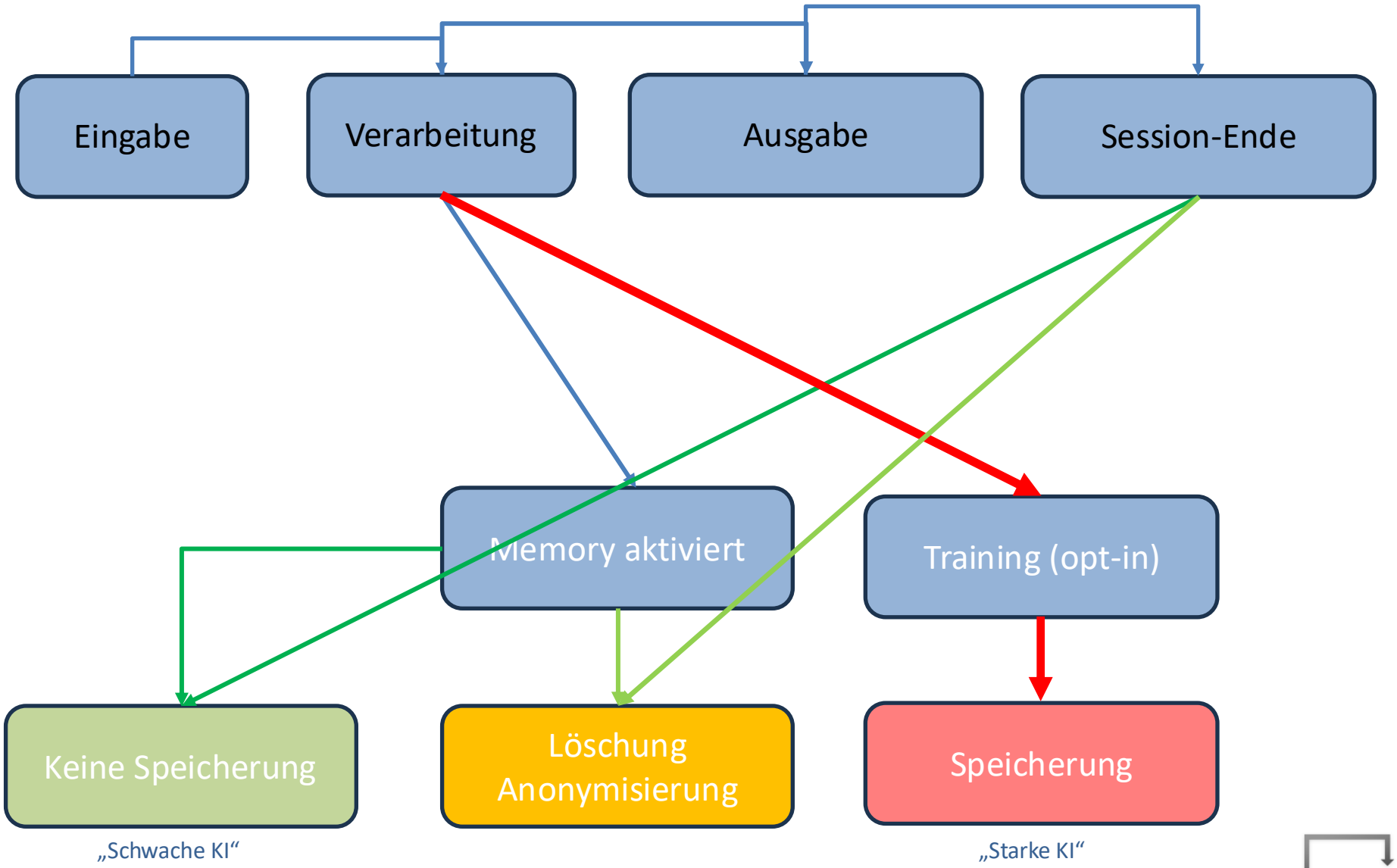
**Bearbeitung im LLM**

Durchforsten
Auseinandernehmen
Verlinken
Analysieren
speichern
Erstellung von internen Algo-rhytmen
Bereithalten
.....

**Bereitstellen**

Datenausgabe
Löschen ?
Zwischenspeicherung?
Trainingsverwendung?
.....

# KI-Aspekte aus rein datenschutzrechtlicher Sicht (3)



# KI-Aspekte aus rein datenschutzrechtlicher Sicht (4)

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 Personenbezug** 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.

# KI-Aspekte aus rein datenschutzrechtlicher Sicht (4)

## 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“?)

**BUNDESARBEITSGERICHT**

8 AZR 209/21
17 Sa 37/20
Landesarbeitsgericht
Baden-Württemberg

**Im Namen des Volkes!**

Verkündet am
8. Mai 2025

**URTEIL**

# BAG-Urteil: Datenschutzverstoß durch Workday-Testsystem

Auch in Deutschland geriet Workday ins Visier der Justiz. In einem Verfahren vor dem Bundesarbeitsgericht (BAG) ging es um die Frage, ob ein Arbeitgeber berechtigt war, die Daten seines Arbeitnehmers in einer Workday-Testumgebung zu verwenden.

Das Gericht kam zu einem klaren Ergebnis: Die Datenverarbeitung entbehrte jeglicher Rechtsgrundlage – also ein fundamentaler Verstoß gegen die Datenschutz-Grundverordnung (DSGVO).

Die Richter betonten, dass selbst eine Betriebsvereinbarung zur Einführung des Systems keine ausreichende Rechtsgrundlage für die konkrete Verarbeitung sensibler Bewerberdaten in einem Testsystem darstellt. Die Folge: Der betroffenen Person wurde Schadensersatz nach Art. 82 DSGVO zugesprochen. Zugleich stellte das Gericht klar, dass auch Testumgebungen den vollen Anforderungen des Datenschutzrechts unterliegen.

(Quelle: https://www.bundesarbeitsgericht.de/presse/schadenersatz-nach-datenschutz-grundverordnung-dsgvo-betriebsvereinbarung-workday/)

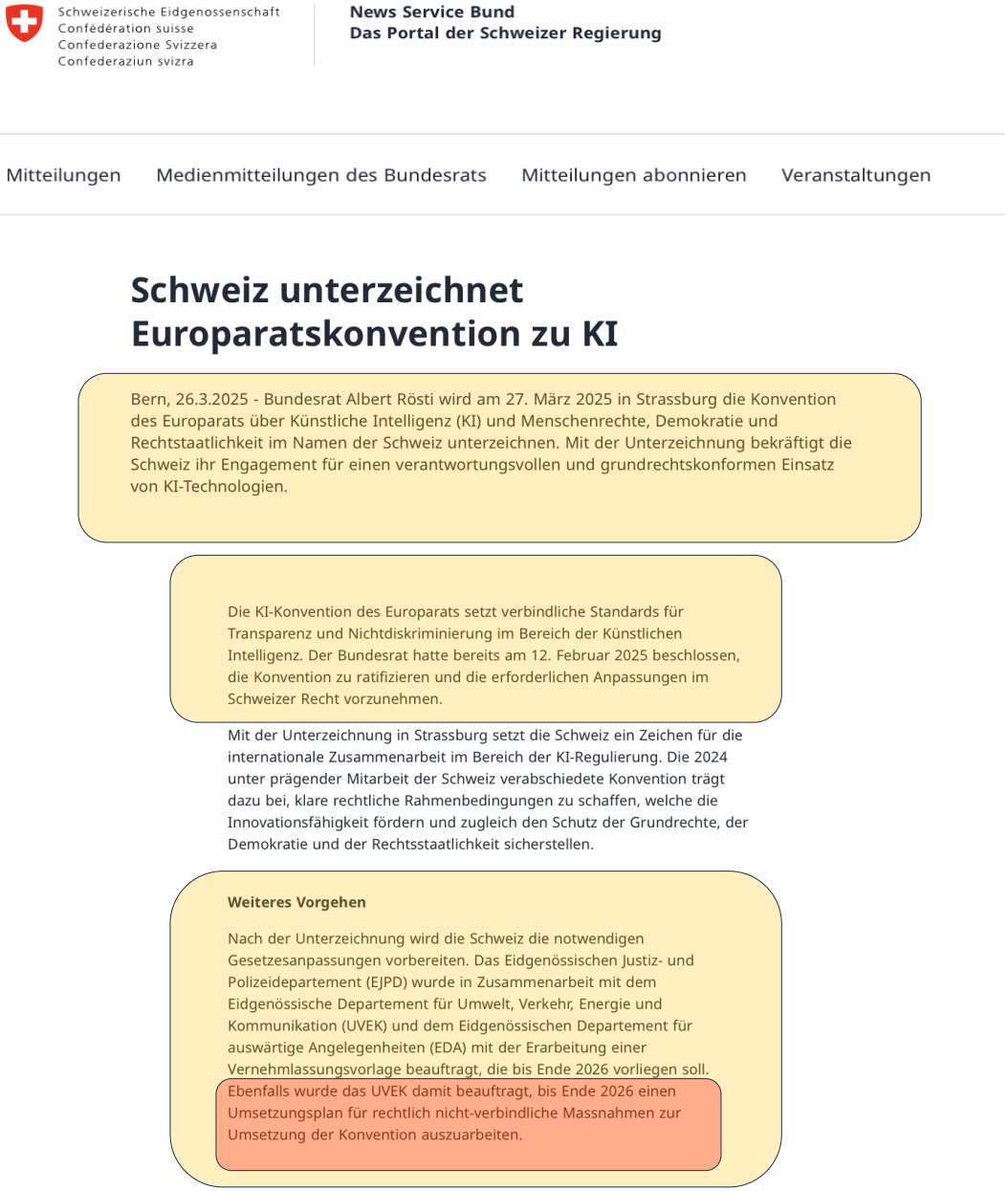
# KI in der Schweiz

Die Schweiz hat Ende März 2025 die Konvention des Europarates über Künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit unterzeichnet. Das bedeutet: Die Schweiz will die Europarats-Konvention ratifizieren und ins Schweizer Recht übernehmen.

Damit sollen Innovationen gefördert, aber Risiken minimiert werden.

Ende 2026 wird eine Vernehmlassungsvorlage erwartet.

# KI-Aspekte aus rein datenschutzrechtlicher Sicht (7)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**News Service Bund**
**Das Portal der Schweizer Regierung**

Mitteilungen | Medienmitteilungen des Bundesrats | Mitteilungen abonnieren | Veranstaltungen

## Schweiz unterzeichnet Europaratskonvention zu KI

Bern, 26.3.2025 - Bundesrat Albert Rösti wird am 27. März 2025 in Strassburg die Konvention des Europarats über Künstliche Intelligenz (KI) und Menschenrechte, Demokratie und Rechtstaatlichkeit im Namen der Schweiz unterzeichnen. Mit der Unterzeichnung bekräftigt die Schweiz ihr Engagement für einen verantwortungsvollen und grundrechtskonformen Einsatz von KI-Technologien.

Die KI-Konvention des Europarats setzt verbindliche Standards für Transparenz und Nichtdiskriminierung im Bereich der Künstlichen Intelligenz. Der Bundesrat hatte bereits am 12. Februar 2025 beschlossen, die Konvention zu ratifizieren und die erforderlichen Anpassungen im Schweizer Recht vorzunehmen.

Mit der Unterzeichnung in Strassburg setzt die Schweiz ein Zeichen für die internationale Zusammenarbeit im Bereich der KI-Regulierung. Die 2024 unter prägender Mitarbeit der Schweiz verabschiedete Konvention trägt dazu bei, klare rechtliche Rahmenbedingungen zu schaffen, welche die Innovationsfähigkeit fördern und zugleich den Schutz der Grundrechte, der Demokratie und der Rechtsstaatlichkeit sicherstellen.

**Weiteres Vorgehen**

Nach der Unterzeichnung wird die Schweiz die notwendigen Gesetzesanpassungen vorbereiten. Das Eidgenössischen Justiz- und Polizeidepartement (EJPD) wurde in Zusammenarbeit mit dem Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) mit der Erarbeitung einer Vernehmlassungsvorlage beauftragt, die bis Ende 2026 vorliegen soll.

Ebenfalls wurde das UVEK damit beauftragt, bis Ende 2026 einen Umsetzungsplan für rechtlich nicht-verbindliche Massnahmen zur Umsetzung der Konvention auszuarbeiten.

# KI-Aspekte aus rein datenschutzrechtlicher Sicht (8)

# KI-Aspekte aus rein datenschutzrechtlicher Sicht (9)

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)**

*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;

Art. 3 Ki-Act

4. „Betreiber“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

## 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/

# KI-Aspekte aus rein datenschutzrechtlicher Sicht (12)

## Handlungsbedarf 2 für CH-Unternehmen

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.

# Wie erkenne ich mit KI erstellte Bewerbungen (13)

Wenn in einem Text **verborgene Sonderzeichen** enthalten sind (z. B. Steuerzeichen, Zero-Width Spaces, unsichtbare Unicode-Zeichen), dann sieht der Text **auf den ersten Blick normal aus** – für das menschliche Auge ist meist kein Unterschied erkennbar.

### Beispiele für „unsichtbare" Zeichen:

- **Zero-Width Space (ZWSP, U+200B)** → wird nicht angezeigt, erzeugt aber einen unsichtbaren Trenner.
- **Zero-Width Non-Joiner (U+200C)** und **Zero-Width Joiner (U+200D)** → steuern die Darstellung von Schriftzeichen, erscheinen aber nicht sichtbar.
- **Non-Breaking Space (U+00A0)** → sieht wie ein normales Leerzeichen aus, ist aber ein anderes Zeichen.
- **Steuerzeichen** (z. B. Tab, Zeilenumbruch, Carriage Return) können im Text verborgen sein.

# Wie erkenne ich mit KI erstellte Bewerbungen (14)

Testdatei.docx
Dokument

bitte zeige mir im beigefügten Text die verborgenen Sonderzeichen

Ich habe mir deine **Testdatei.docx** angeschaut.
Darin stecken tatsächlich **unsichtbare Sonderzeichen** – hier die Übersicht:

---

### 🔎 Gefundene verborgene Zeichen

1. **Satz 1 – „Heute gehe ichspazieren."**
   → Enthält ein **Zero-Width Space (U+200B)** zwischen „ich" und „spazieren".
2. **Satz 7 – „Zero-Width-Spacehier."**
   → Zwischen „Space" und „hier" steckt ebenfalls ein **Zero-Width Space (U+200B)**.
3. **Satz 8 – „Non-Breaking-Hyphen"**
   → Das Bindestrich-Zeichen ist kein normales Minus (U+002D), sondern ein **Non-Breaking Hyphen (U+2011)**.

---

### ✅ Keine unsichtbaren Zeichen gefunden in:

- Den Sätzen 2, 3, 4, 5, 6, 9 und 10.
  (Dort sind nur „sichtbare" Zeichen wie Umlaute `ö, ä, ü` enthalten, aber keine Zero-Width- oder Sonder-Leerzeichen.)

# Wie erkenne ich mit KI erstellte Bewerbungen (15)

soscisurvey.de/tools/view-chars.php

## View non-printable unicode characters

Online tool to display non-printable characters that may be hidden in copy&pasted strings.

Please paste the string here:

Kritik, da er Umweltauflagen für Fabriken lockert und die EPA (Umweltschutzbehörde) umstrukturiertfaz.net.
Innenpolitisch sorgt Trump mit seiner Rhetorik und der Instrumentalisierung von Gewaltvorfällen für Aufsehen: Nach dem tödlichen Angriff auf den konservativen Aktivisten Charlie Kirk machte er die politische Opposition öffentlich verantwortlichtagesschau.de+1. Seine juristischen Auseinandersetzungen halten an, unter anderem mit Klagen gegen Medien und laufenden Berufungsverfahren in früheren Zivilprozessenen.wikipedia.org. Trotz seiner Versprechen, die Wirtschaft zu stärken, sinkt seine Zustimmung in der Bevölkerung, da viele Amerikaner die versprochenen Lohnerhöhungen und sinkende Inflation nicht spüreneconomist.com.
Trump bleibt eine umstrittene Figur, die mit provokanten Aussagen und unkonventionellen Methoden die politische Landschaft der USA prägt. Seine Anhänger sehen in ihm einen starken Führer, während seine Gegner die Spaltung des Landes und die Schwächung internationaler Bündnisse kritisierenfaz.net+2.

Show me the characters

See U+A0 what's·hidden·in·your·string…⟶or·be U+200B hind U+FEFF

45 characters, 52 bytes

# Wie erkenne ich mit KI erstellte Bewerbungen (16)

## View non-printable unicode characters

Online tool to display non-printable characters that may be hidden in copy&pasted strings.

Please paste the string here:

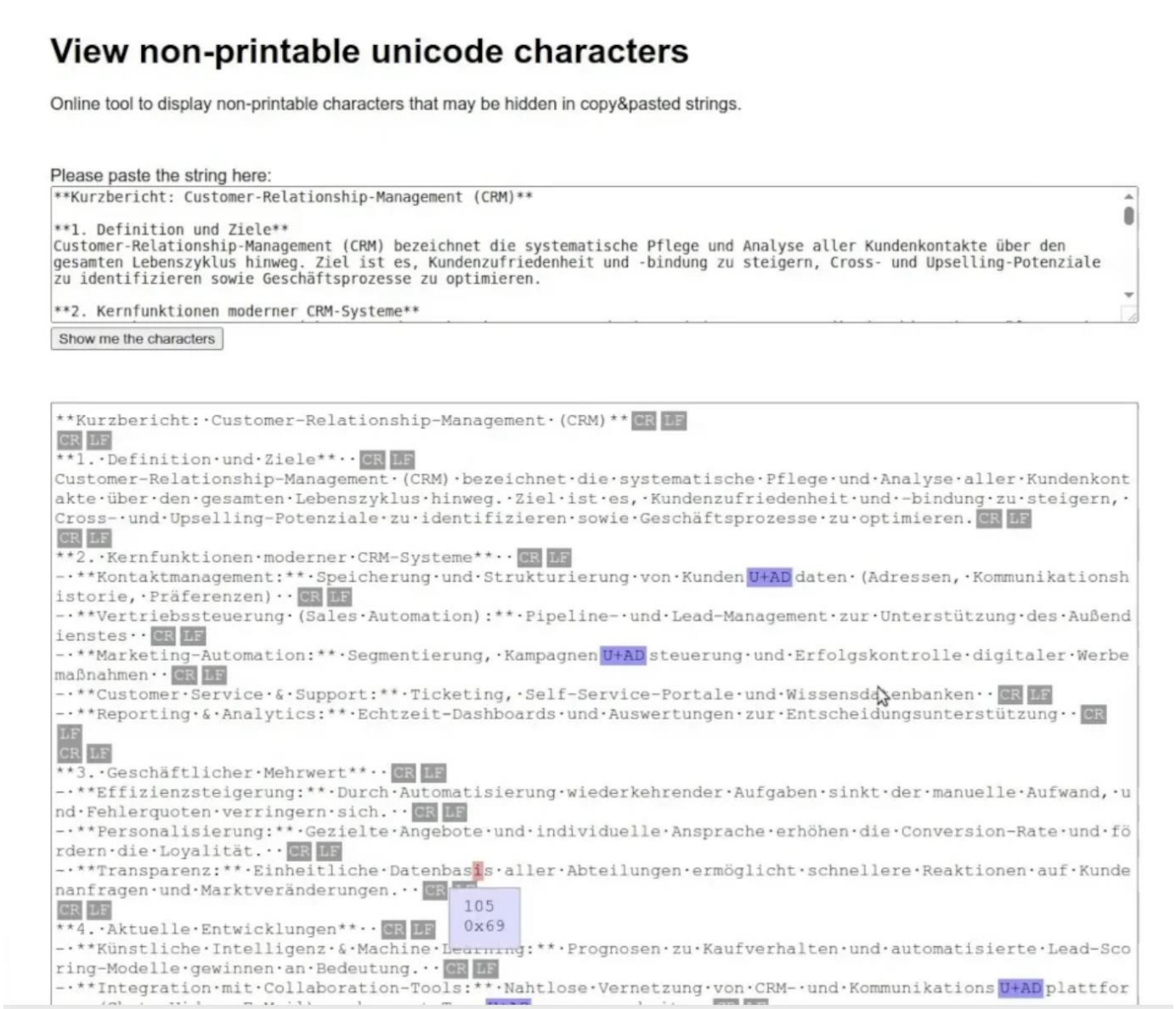
Donald Trump ist seit Januar 2025 zum zweiten Mal US-Präsident und führt das Land mit einer klar polarisierenden Agenda. In seiner zweiten Amtszeit setzt er weiterhin auf eine harte Handelspolitik, etwa durch hohe Zölle auf Importe aus China und Europa, was weltweit für wirtschaftliche Spannungen sorgtfoxnews.com+1. Trump fordert die NATO-Staaten auf, ihre Ölkäufe aus Russland einzustellen, bevor er bereit ist, neue Sanktionen gegen Moskau zu verhängen – eine Forderung, die in Europa auf Kritik stößtzeit.de+1. Seine Klimapolitik steht in der Kritik, da er Umweltauflagen für Fabriken lockert und die EPA (Umweltschutzbehörde) umstrukturiertfaz.net.
Innenpolitisch sorgt Trump mit seiner Rhetorik und der Instrumentalisierung von Gewaltvorfällen für Aufsehen: Nach dem tödlichen Angriff auf den konservativen Aktivisten Charlie Kirk machte er die politische Opposition öffentlich verantwortlichtagesschau.de+1. Seine juristischen Auseinandersetzungen halten an, unter anderem mit Klagen gegen Medien und laufenden Berufungsverfahren in früheren Zivilprozessenen.wikipedia.org. Trotz seiner Versprechen, die Wirtschaft zu stärken, sinkt seine Zustimmung in der Bevölkerung, da viele Amerikaner die versprochenen Lohnerhöhungen und sinkende Inflation nicht spüreneconomist.com.

Show me the characters

Donald·Trump·ist·seit·Januar·2025·zum·zweiten·Mal·US-Präsident·und·führt·das·Land·mit·einer·klar·
polarisierenden·Agenda.·In·seiner·zweiten·Amtszeit·setzt·er·weiterhin·auf·eine·harte·Handelspolitik,·
etwa·durch·hohe·Zölle·auf·Importe·aus·China·und·Europa,·was·weltweit·für·wirtschaftliche·Spannungen·
sorgtfoxnews.com+1.·Trump·fordert·die·NATO-Staaten·auf,·ihre·Ölkäufe·aus·Russland·einzustellen,·bevor·
er·bereit·ist,·neue·Sanktionen·gegen·Moskau·zu·verhängen·–·eine·Forderung,·die·in·Europa·auf·Kritik·
stößtzeit.de+1.·Seine·Klimapolitik·steht·in·der·Kritik,·da·er·Umweltauflagen·für·Fabriken·lockert·und·
die·EPA·(Umweltschutzbehörde)·umstrukturiertfaz.net.CR LF
Innenpolitisch·sorgt·Trump·mit·seiner·Rhetorik·und·der·Instrumentalisierung·von·Gewaltvorfällen·für·
Aufsehen:·Nach·dem·tödlichen·Angriff·auf·den·konservativen·Aktivisten·Charlie·Kirk·machte·er·die·
politische·Opposition·öffentlich·verantwortlichtagesschau.de+1.·Seine·juristischen·
Auseinandersetzungen·halten·an,·unter·anderem·mit·Klagen·gegen·Medien·und·laufenden·Berufungsverfahren·
in·früheren·Zivilprozessenen.wikipedia.org.·Trotz·seiner·Versprechen,·die·Wirtschaft·zu·stärken,·sinkt·
seine·Zustimmung·in·der·Bevölkerung,·da·viele·Amerikaner·die·versprochenen·Lohnerhöhungen·und·sinkende·
Inflation·nicht·spüreneconomist.com.CR LF
Trump·bleibt·eine·umstrittene·Figur,·die·mit·provokanten·Aussagen·und·unkonventionellen·Methoden·die·
politische·Landschaft·der·USA·prägt.·Seine·Anhänger·sehen·in·ihm·einen·starken·Führer,·während·seine·
Gegner·die·Spaltung·des·Landes·und·die·Schwächung·internationaler·Bündnisse·kritisierenfaz.net+2.CR LF
U+FEFF

1585 characters, 1615 bytes

# Wie erkenne ich mit KI erstellte Bewerbungen (17)



## View non-printable unicode characters

Online tool to display non-printable characters that may be hidden in copy&pasted strings.

Please paste the string here:

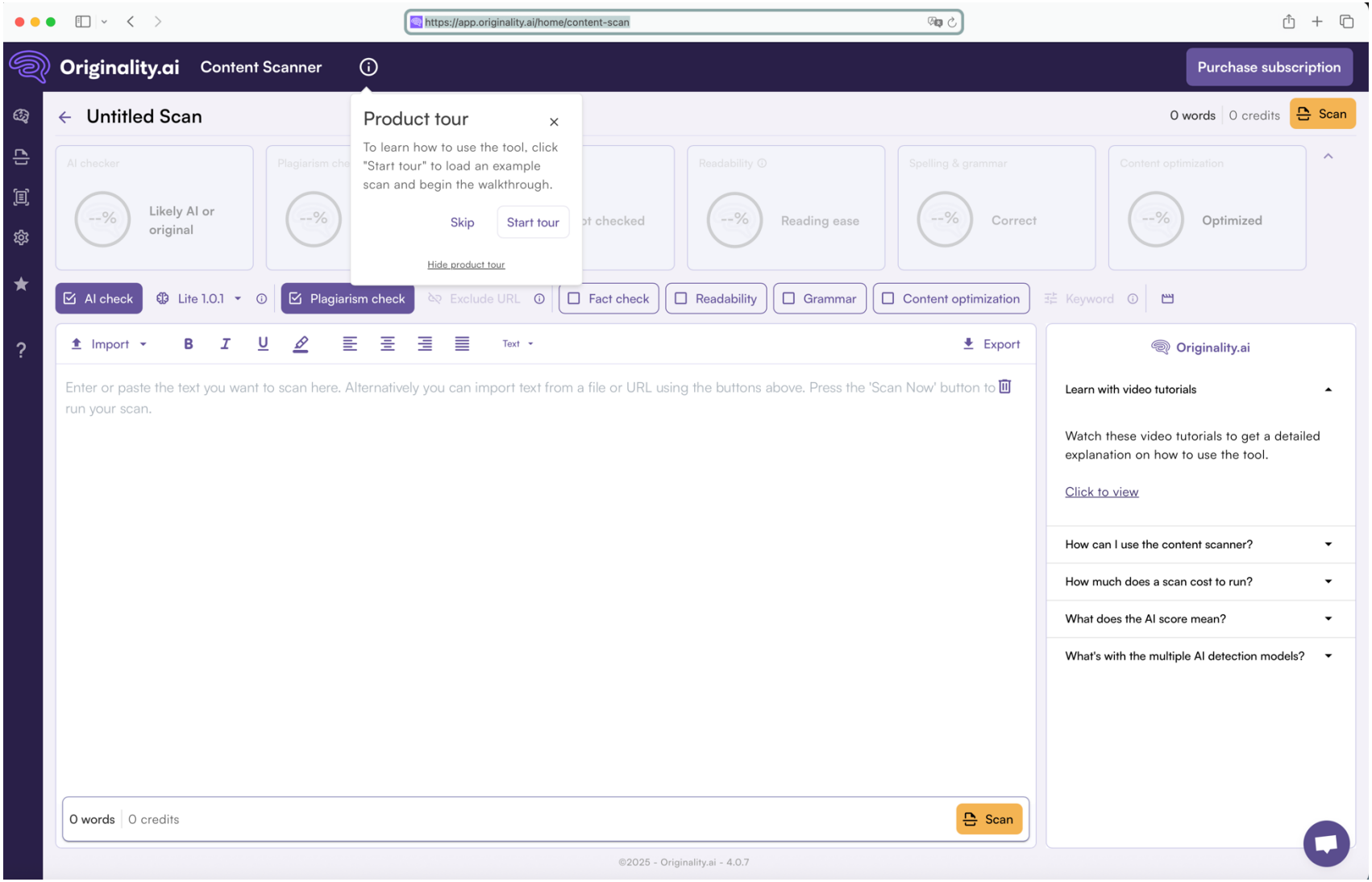
```
**Kurzbericht: Customer-Relationship-Management (CRM)**

**1. Definition und Ziele**
Customer-Relationship-Management (CRM) bezeichnet die systematische Pflege und Analyse aller Kundenkontakte über den
gesamten Lebenszyklus hinweg. Ziel ist es, Kundenzufriedenheit und -bindung zu steigern, Cross- und Upselling-Potenziale
zu identifizieren sowie Geschäftsprozesse zu optimieren.

**2. Kernfunktionen moderner CRM-Systeme**
```

Show me the characters

```
**Kurzbericht:·Customer-Relationship-Management·(CRM)**CR LF
CR LF
**1.·Definition·und·Ziele**··CR LF
Customer-Relationship-Management·(CRM)·bezeichnet·die·systematische·Pflege·und·Analyse·aller·Kundenkont
akte·über·den·gesamten·Lebenszyklus·hinweg.·Ziel·ist·es,·Kundenzufriedenheit·und·-bindung·zu·steigern,·
Cross-·und·Upselling-Potenziale·zu·identifizieren·sowie·Geschäftsprozesse·zu·optimieren.CR LF
CR LF
**2.·Kernfunktionen·moderner·CRM-Systeme**··CR LF
-·**Kontaktmanagement:**·Speicherung·und·Strukturierung·von·KundenU+ADdaten·(Adressen,·Kommunikationsh
istorie,·Präferenzen)··CR LF
-·**Vertriebssteuerung·(Sales·Automation):**·Pipeline-·und·Lead-Management·zur·Unterstützung·des·Außend
ienstes··CR LF
-·**Marketing-Automation:**·Segmentierung,·KampagnenU+ADsteuerung·und·Erfolgskontrolle·digitaler·Werbe
maßnahmen··CR LF
-·**Customer·Service·&·Support:**·Ticketing,·Self-Service-Portale·und·Wissensdatenbanken··CR LF
-·**Reporting·&·Analytics:**·Echtzeit-Dashboards·und·Auswertungen·zur·Entscheidungsunterstützung··CR
LF
CR LF
**3.·Geschäftlicher·Mehrwert**··CR LF
-·**Effizienzsteigerung:**·Durch·Automatisierung·wiederkehrender·Aufgaben·sinkt·der·manuelle·Aufwand,·u
nd·Fehlerquoten·verringern·sich.··CR LF
-·**Personalisierung:**·Gezielte·Angebote·und·individuelle·Ansprache·erhöhen·die·Conversion-Rate·und·fö
rdern·die·Loyalität.··CR LF
-·**Transparenz:**·Einheitliche·Datenbasis·aller·Abteilungen·ermöglicht·schnellere·Reaktionen·auf·Kunde
nanfragen·und·Marktveränderungen.··CR
105
0x69
CR LF
**4.·Aktuelle·Entwicklungen**··CR LF
-·**Künstliche·Intelligenz·&·Machine·Learning:**·Prognosen·zu·Kaufverhalten·und·automatisierte·Lead-Sco
ring-Modelle·gewinnen·an·Bedeutung.··CR LF
-·**Integration·mit·Collaboration-Tools:**·Nahtlose·Vernetzung·von·CRM-·und·Kommunikations U+ADplattfor
```

# Wie erkenne ich mit KI erstellte Bewerbungen (18)

## z.B. Erkennen von Plagiaten



# Fazit: ChatGPT Wasserzeichen – Mythos oder Realität?

Zusammenfassend lässt sich sagen, dass das sogenannte ChatGPT Wasserzeichen kein bewusstes, technisches Wasserzeichen ist, sondern eher eine Folge der Trainingsdaten und der Textausgabe mit Soft Hyphens. Diese bedingten Trennstriche sind in vielen Webtexten üblich und werden von ChatGPT übernommen.

Die Erkennung dieser Unicode-Zeichen kann ein erster Hinweis darauf sein, dass ein Text von ChatGPT generiert wurde. Allerdings ist diese Methode nicht narrensicher und funktioniert nur bei Texten, die diese Sonderzeichen enthalten.

Andere KI-Textdetektoren wie ZeroGPT funktionieren aktuell nur begrenzt zuverlässig, vor allem bei modernen Modellen. Die KI-Entwicklung schreitet schnell voran, was die Erkennung immer schwieriger macht.

Mehr über den rechtskonformen und auch ethischen Einsatz von KI erfahren Sie in unserer Blog-Serie:

- [Teil 1: KI am Arbeitsplatz: Die drei wichtigsten Punkte für Mitarbeitende](https://www.vischer.com/de/insights/teil-1-ki-am-arbeitsplatz-die-drei-wichtigsten-* Teil 1: KI am Arbeitsplatz: Die drei wichtigsten Punkte für Mitarbeitende
- Teil 2: Gängige KI-Tools: Wie steht es um den Datenschutz?
- Teil 3: KI: 11 Grundsätze – und eine Weisung für Mitarbeitende
- Teil 4: So beurteilen Sie Risiken von kleinen und grossen KI-Projekten
- Teil 5: KI-Governance im Unternehmen – wer ist verantwortlich?
- Teil 6: Die andere Seite der Medaille: Wo wir KI vor Angreifern schützen müssen
- Teil 7: Der EU AI Act – und was er für die meisten Unternehmen bedeutet
- Teil 8: KI im Finanzinstitut – Chancen und Herausforderungen
- Teil 9: KI im Marketing: 4 wettbewerbsrechtliche Fallstricke
- Teil 10: Urheberrecht und KI: Verantwortlichkeit von Anbietern und Nutzern
- Teil 11: Fair Play mit KI: Wie Sportorganisationen Athletendaten nutzen dürfen
- Teil 12: Datenfutter für KI: So gelingt die Kommerzialisierung von Datensätzen
- Teil 13: KI im Personalwesen
- Teil 14: Urheberrecht und KI: Schutzmassnahmen in der Praxis
- Teil 15: Worauf rechtlich beim Einsatz von KI-Providern zu achten ist
- Teil 16: Wie Unternehmen beim Einsatz von KI Transparenz gewährleisten können
- Teil 17: Was in einem KI-Modell steckt und wie es funktioniert
- Teil 18: Die wichtigsten Compliance-Vorgaben für KI
- Teil 19: Sprachmodelle mit und ohne personenbezogene Daten
- Teil 20: Risiko-basierter Ansatz: Nicht alle KI-Anwendungen bergen hohe Risiken
- Teil 21: Das Auskunftsrecht bei grossen Sprachmodellen
- Teil 22: Leitsätze für den Einsatz künstlicher Intelligenz in Finanzinstituten (FINMA)
- Teil 23: Schweiz: Was konkret an KI-Regulierung zu erwarten ist

https://www.vischer.com/de/artificial-intelligence

Mehr über den rechtskonformen und auch ethischen Einsatz von KI erfahren Sie in unserer Blog-Serie:

- [Teil 1: KI am Arbeitsplatz: Die drei wichtigsten Punkte für Mitarbeitende](https://www.vischer.com/de/insights/teil-1-ki-am-arbeitsplatz-die-drei-wichtigsten-* Teil 1: KI am Arbeitsplatz: Die drei wichtigsten Punkte für Mitarbeitende
- Teil 2: Gängige KI-Tools: Wie steht es um den Datenschutz?
- Teil 3: KI: 11 Grundsätze – und eine Weisung für Mitarbeitende
- Teil 4: So beurteilen Sie Risiken von kleinen und grossen KI-Projekten
- Teil 5: KI-Governance im Unternehmen – wer ist verantwortlich?
- Teil 6: Die andere Seite der Medaille: Wo wir KI vor Angreifern schützen müssen
- Teil 7: Der EU AI Act – und was er für die meisten Unternehmen bedeutet
- Teil 8: KI im Finanzinstitut – Chancen und Herausforderungen
- Teil 9: KI im Marketing: 4 wettbewerbsrechtliche Fallstricke
- Teil 10: Urheberrecht und KI: Verantwortlichkeit von Anbietern und Nutzern
- Teil 11: Fair Play mit KI: Wie Sportorganisationen Athletendaten nutzen dürfen
- Teil 12: Datenfutter für KI: So gelingt die Kommerzialisierung von Datensätzen
- Teil 13: KI im Personalwesen
- Teil 14: Urheberrecht und KI: Schutzmassnahmen in der Praxis
- Teil 15: Worauf rechtlich beim Einsatz von KI-Providern zu achten ist
- Teil 16: Wie Unternehmen beim Einsatz von KI Transparenz gewährleisten können
- Teil 17: Was in einem KI-Modell steckt und wie es funktioniert
- Teil 18: Die wichtigsten Compliance-Vorgaben für KI
- Teil 19: Sprachmodelle mit und ohne personenbezogene Daten
- Teil 20: Risiko-basierter Ansatz: Nicht alle KI-Anwendungen bergen hohe Risiken
- Teil 21: Das Auskunftsrecht bei grossen Sprachmodellen
- Teil 22: Leitsätze für den Einsatz künstlicher Intelligenz in Finanzinstituten (FINMA)
- Teil 23: Schweiz: Was konkret an KI-Regulierung zu erwarten ist

https://www.vischer.com/de/artificial-intelligence

# Compliance-Grundsätze für KI-Einsatz (19)


https://www.vischer.com/know-how/blog/teil-1-ki-am-arbeitsplatz-die-drei-wichtigsten-punkte-fuer-mitarbeitende/

# Compliance-Grundsätze für KI-Einsatz (20)

## Punkt Nr. 1

Eine KI versteht nicht

Ihre Antworten können voreingenommen, ungenau oder erfunden sein

Darum: Prüfe das Ergebnis

Du bleibst verantwortlich

Nutze KI, aber behalte die Kontrolle

VISCHER
SWISS LAW AND TAX

https://www.vischer.com/know-how/blog/teil-1-ki-am-arbeitsplatz-die-drei-wichtigsten-punkte-fuer-mitarbeitende/

# Compliance-Grundsätze für KI-Einsatz (21)

## Punkt Nr. 2

Nicht alle Anbieter sind vertrauenswürdig

Geheimnisse, Daten über andere und Inhalte Dritter nur in den dafür freigegebenen KI-Systemen verwenden

Lerne den Umgang mit KI, damit Du ihre Grenzen verstehst

VISCHER
SWISS LAW AND TAX

https://www.vischer.com/know-how/blog/teil-1-ki-am-arbeitsplatz-die-drei-wichtigsten-punkte-fuer-mitarbeitende/

# Compliance-Grundsätze für KI-Einsatz (22)

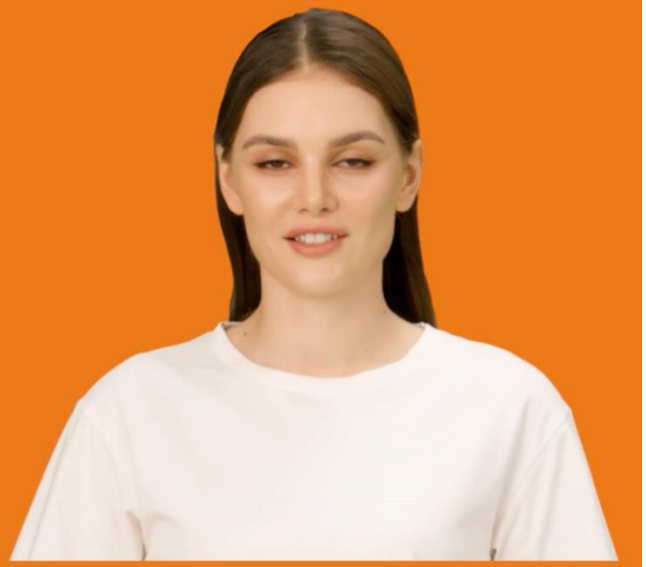
## Punkt Nr. 3

Viele Regeln gibt es schon

Höre auf Dein Gefühl –
fühlt es sich richtig an?

Prüfe Dein KI-Vorhaben
frühzeitig mit Euren
Fachleuten

Diskutiert Eure ethischen Prinzipien



VISCHER
SWISS LAW AND TAX

https://www.vischer.com/know-how/blog/teil-1-ki-am-arbeitsplatz-die-drei-wichtigsten-punkte-fuer-mitarbeitende/

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).

# Konkrete Massnahmen

- **Umsetzung der neuen Datensicherheitsvorgaben gemäss CH-DSG**
  - Dateninventar, Bearbeitungsverzeichnis, Datenschutzfolgeabschätzung, techn. und organ. Massnahmen (TOM‘s), Verträge mit Datenverarbeitern
- **Prozessbeschreibungen** für
  - Wahrung der Rechte der Betroffenen (Kunden, Lieferanten etc.)
  - Meldepflichten an Datenschutzbehörde
  - Benachrichtigungen an Betroffene
- **Jährliche Überprüfung der Cyberrisiko-Situation und der TOM‘s**
  - GAP-Analyse in GL vorbereiten und mit VR abstimmen
  - Standard-Traktandum 1x jährlich Analyse und Beschlüsse protokollieren
- **Awareness-Schulungen der Mitarbeitenden (Nachweise)**

# Konkrete Massnahmen bei KI-Einsatz

# Aufgabe

Erstellen Sie mit Hilfe einer KI-Plattform (ohne Abonnemente; Billig- oder Testversionen) einen ersten **Entwurf zu einer Weisung für den KI-Einsatz und die Nutzung von KI durch Mitarbeitende** in Ihrem Unternehmen.

ChatGPT

https://chatgpt.com

Mistral AI

https://mistral.ai

Gemini

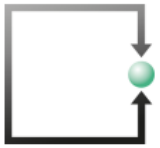
https://gemini.google.com/app

Claude

https://claude.ai/new

deepcloud

https://www.deepcloud.swiss



Rechtsanwälte
ATTORNEYS @ LAW

# FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

Impressum Datenschutzbestimmungen

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

## Aktuelles aus unserer Kanzlei.

Alle | Intern | Publikationen | Veranstaltungen

### CAS Information-Security und Risk-Management

**Verfasst am 29.05.2019**
Fachhochschule Nordwest-Schweiz, FHNW in Basel

Rechtsanwalt Lukas Fässler unterrichtet an der FHNW in Basel. In diesem Kursmodul werden aus der Sicht IT-Sicherheit und IT-Riskmanagement folgende Aspekte beleuchtet:

Grundsätze der Unternehmensführung
Coperate Governance und Complianc
Grundsätze von Datenschutz und neues Datenschutzrecht (DSGVO und E-DSG Schweiz)
Grundsätze von IT-Sicherheit
Schadensbegrenzung und Abwägung
››Weiterlesen

### Datenschutz und Datensicherheit in der Arztpraxis

**Verfasst am 16.05.2019**

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben


FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
Fax +41 41 727 60 85
sekretariat@fsdz.ch
Karte Google Maps

Rechtsanwalt
lic. iur. Lukas Fässler
Telefon +41 41 727 60 80
Mobile +41 79 209 24 32
faessler@fsdz.ch

Rechtsanwältin und Notarin
lic. iur. Carmen de la Cruz Böhringer
Telefon +41 41 727 60 80
sekretariat@fsdz.ch

# Besten Dank

**Lukas Fässler**

Rechtsanwalt & Informatikexperte
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76B
CH-6340 Baar
Tel. +41 +41 727 60 80
www.fsdz.ch
faessler@fsdz.ch

# Grundlagen für eine KI-Weisung in einer KMU

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# KI im Personalwesen – zentrale Einsatzfelder

Potenziale entlang des gesamten HR-Prozesses – mit menschlicher Prüfung und Entscheidung

## 1 Recruiting & Talentakquise

- Stellenprofile & Anforderungsprofile erstellen
- CV-Screening und Shortlists vorbereiten
- Vorgespräche & personalisierte Interviewfragen
- Interviewanalyse und Bewerberkommunikation

## 2 Personalentwicklung & Schulung

- Personalisierte Lern- und Schulungspläne
- Automatisierte Lernpfade
- Weiterbildungsempfehlungen nach Skills & Interessen

## 3 Engagement & Bindung

- Feedback analysieren und Trends erkennen
- Verbesserungsfelder identifizieren
- Individuelle Karriere- und Lernempfehlungen

## 4 Performance Management

- Leistungsdaten analysieren
- Hinweise und Erinnerungen für Reviews automatisieren

## 5 Mitarbeiterdaten & Administration

- Datenerfassung und -verarbeitung automatisieren
- Unterstützung bei Einstellung, Beförderung und Mutationen

**Kernprinzip: KI unterstützt HR-Fachpersonen bei Analyse, Vorbereitung und Automatisierung – Auswahl- und Personalentscheide bleiben menschlich.**



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Vorteile des Einsatzes von KI im Personalwesen

KI unterstützt HR bei Automatisierung, Analyse, Personalisierung und Mitarbeiterbetreuung

01

## Effizienz

Repetitive Aufgaben automatisieren

→ mehr Zeit für strategische HR-Arbeit

02

## Entscheidungsgrundlagen

Grosse Datenmengen analysieren

→ Muster erkennen und Entscheidungen fundieren

03

## Personalisierung

Individuelle Lern-, Weiterbildungs- und Karriereempfehlungen

04

## Objektivität

Datenbasierte Prozesse

→ Potenzial zur Reduktion von Bias und Diskriminierung

05

## Talent & Bindung

Talente gezielter identifizieren

→ Engagement durch personalisierte Ansätze stärken

06

## Zeitersparnis

Automatisierung von Terminierung, Onboarding und Offboarding

07

## Mitarbeitererfahrung

KI-Chatbots als jederzeit verfügbare Unterstützung bei HR-Fragen

08

## Leistungsmanagement

Leistungsdaten analysieren

→ frühzeitig auf Auffälligkeiten hinweisen

**Kernaussage: KI kann HR effektiver und datenorientierter machen – mit Potenzial für mehr Zeit, Qualität und eine bessere Mitarbeitererfahrung.**



FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Nachteile und Risiken von KI im Personalwesen

Technologie kann HR unterstützen – sie ersetzt aber weder Verantwortung noch menschliches Urteil.

1

## Mensch & Transparenz

Weniger persönlicher Kontakt kann Distanz schaffen. Black-Box-Modelle erschweren die Nachvollziehbarkeit von HR-Entscheidungen.

2

## Vorurteile & Diskriminierung

Historische Daten können bestehende Verzerrungen reproduzieren. Modelle und Resultate müssen regelmässig auf Benachteiligungen geprüft werden.

3

## Datenschutz & Sicherheit

HR-KI verarbeitet sensible Personendaten. Datenlecks, unbefugte Zugriffe und unklare Weiterverwendung erhöhen das Schutzbedürfnis.

4

## Fehlende Intuition

KI erkennt Muster, verfügt aber nicht über menschliche Empathie, Kontextverständnis oder emotionale Intelligenz.

5

## Technische Fehler

Fehlerhafte Daten, Modelle oder Systemausfälle können zu falschen Empfehlungen und Entscheidungen führen.

6

## Akzeptanz & Aufwand

Widerstand, Arbeitsplatzängste sowie Investitionen in Technik, Schulung, Governance und Prozesse können die Einführung erschweren.

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

Konsequenz für HR:

# KI braucht klare Leitplanken.

Der Nutzen entsteht erst, wenn Technologie, Recht, Prozesse und menschliche Verantwortung zusammenspielen.

Kernbotschaft

**KI als Entscheidungsunterstützung – nicht als unkontrollierter Entscheider.**

01

## Human-in-the-loop

Wesentliche Personalentscheide nicht unkontrolliert an KI delegieren; menschliche Überprüfung sicherstellen.

02

## Transparenz

Zweck, Datenquellen und Funktionsweise verständlich dokumentieren und Betroffene angemessen informieren.

03

## Bias-Kontrollen

Trainingsdaten, Modelle und Ergebnisse regelmässig auf systematische Benachteiligungen testen.

04

## Datenschutz by Design

Datenminimierung, Zugriffsschutz, Zweckbindung und – bei hohem Risiko – Datenschutz-Folgenabschätzung einplanen.

05

## Governance & Resilienz

Verantwortlichkeiten, Freigaben, Monitoring, Schulungen sowie Verfahren für Fehler und Ausfälle definieren.

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

KÜNSTLICHE INTELLIGENZ IM PERSONALWESEN

# Rechtliche Rahmenbedingungen

Der Einsatz von KI im HR-Bereich unterliegt bereits heute klaren rechtlichen Vorgaben – insbesondere dem Datenschutzrecht.

Das Datenschutzrecht ist auf KI-gestützte Behandlungen von Personendaten anwendbar – unabhängig davon, ob es sich um Bewerberinnen, Bewerber oder Mitarbeitende handelt.

§

## Information

- Beschäftigte sowie Bewerberinnen und Bewerber müssen vor der Verarbeitung ihrer Daten durch KI-Tools ausreichend informiert werden.
- Transparente Kommunikation über den Einsatz von KI im HR-Bereich.

## Transparenz

- KI-Modelle sind oft komplex und schwer nachvollziehbar.
- Unternehmen sollten offenlegen, wie KI im HR eingesetzt wird und welche Datenquellen verwendet werden – für mehr Vertrauen.

## Automatisierte Entscheidungen

- Vollautomatisierte Entscheidungen im Arbeitsverhältnis sind begrenzt zulässig.
- Bei wichtigen Einzelentscheiden (z. B. Auswahl oder Bewertung) ist menschliches Gehör zwingend.
- Auch vorbereitende KI-Entscheide unterliegen höheren Transparenz-anforderungen.

## Datenschutz-Folgenabschätzung

- Bei bestimmten KI-Anwendungen im HR-Bereich ist eine Datenschutz-Folgenabschätzung (DSFA) erforderlich.
- Diese bewertet mögliche Risiken der Datenverarbeitung für die betroffene Person.

## Datensicherheit

- KI erfordert die Verarbeitung grosser Mengen personenbezogener Daten.
- Daten müssen sicher gespeichert und vor unbefugtem Zugriff geschützt werden – auch bei Einsatz von externen Providern (z. B. Cloud).
- Es sind angemessene vertragliche Regelungen mit den Providern erforderlich.

## Rechte der Betroffenen

- Bewerberinnen, Bewerber und Mitarbeitende haben u. a. das Recht auf:
  - Auskunft über die Verarbeitung ihrer Daten
  - Berichtigung unrichtiger Daten
  - Löschung oder Anonymisierung
- Unternehmen müssen sicherstellen, dass diese Rechte respektiert und effektiv umgesetzt werden.

## Vermeidung von Diskriminierung

- KI-Modelle können unbewusste Voreingenommenheiten aufweisen.
- Unternehmen müssen sicherstellen, dass keine diskriminierenden Entscheidungen getroffen werden (z. B. aufgrund von Geschlecht, ethnischer Zugehörigkeit oder anderen geschützten Merkmalen).
- Regelmässige Überprüfung und Monitoring sind notwendig.


**Fazit:** KI im HR ist rechtlich möglich – aber nur mit klaren Leitplanken.

Datenschutz | Transparenz | Fairness | Menschliche Letztentscheidung



FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Datenschutz bleibt der rechtliche Ausgangspunkt

KI im HR darf Personendaten nur fair, transparent, sicher und gesetzeskonform bearbeiten.

- Zweckbindung, Verhältnismässigkeit und Transparenz gelten auch bei KI-gestützten HR-Prozessen.
- Bei hohem Risiko ist vorab eine Datenschutz-Folgenabschätzung erforderlich.
- Bei automatisierten Einzelentscheidungen bestehen besondere Informations- und Anhörungsrechte.
- Verantwortung und Kontrolle verbleiben beim Arbeitgeber, auch beim Einsatz externer Anbieter.

| Kernaussage | **Datenschutz ist Voraussetzung für faire und nachvollziehbare HR-Entscheide.** |
|---|---|

Quellen: DSG (SR 235.1), Art. 6, 19, 21, 22 und 25; OR, Art. 328b. Fedlex: https://www.fedlex.admin.ch/eli/cc/2022/491/de



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

7

# Wann erfasst der EU AI Act ein Schweizer Unternehmen?

Der Sitz in der Schweiz schliesst die Anwendung des AI Act nicht aus.

## A EU-Marktbezug

Ein Schweizer Anbieter bringt ein KI-System oder KI-Modell in der EU in Verkehr.

## B Einsatz in der EU

Ein Schweizer Unternehmen setzt das KI-System als Betreiber innerhalb der EU ein.

## C Output in der EU

Der in der Schweiz erzeugte Output wird in der EU verwendet, etwa für eine dortige Personalentscheidung.

**Einordnung für die Praxis**

**Bleibt ein Schweizer HR-Prozess vollständig ausserhalb der EU und wird sein Output dort nicht verwendet, greift Art. 2 Abs. 1 lit. c in der Regel nicht. Andere Anknüpfungspunkte müssen dennoch separat geprüft werden.**

Quelle: Verordnung (EU) 2024/1689 (AI Act), Art. 2 Abs. 1 lit. a–c. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# HR-Systeme können als Hochrisiko-KI gelten

Massgebend sind der vorgesehene Zweck und der konkrete Einfluss auf die Personalentscheidung.

## Typische Hochrisiko-Fälle

- Analyse und Filterung von Bewerbungen
- Bewertung oder Rangfolge von Kandidatinnen und Kandidaten
- Entscheide über Beförderung, Kündigung oder Aufgabenzuteilung
- Leistungs- und Verhaltensüberwachung

Rechtsfolge

## Zusätzliche Anforderungen an Hochrisiko-KI

| | |
|---|---|
| **Risikomanagement und Datenqualität** | Art. 9 und 10 |
| **Dokumentation, Protokollierung und Transparenz** | Art. 11–13 |
| **Menschliche Aufsicht, Genauigkeit und Cybersicherheit** | Art. 14 und 15 |
| **Pflichten des Betreibers, einschliesslich Information am Arbeitsplatz** | Art. 26 |

Quellen: AI Act, Art. 6 Abs. 2–3, Art. 8–15, Art. 26 sowie Anhang III Ziff. 4; EU-Kommission, AI Act – High-risk systems (Stand 16.09.2026): https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

ERSTENTWURF

# KI-Weisung für ein Schweizer KMU

Sorgfaltspflichten, Governance und verbindliche Handlungsvorgaben für Mitarbeitende

**Leitgedanke** **KI unterstützt Menschen. Verantwortung und Letztentscheidung bleiben beim Unternehmen.**

Version 0.1 | Rechtsstand 16. September 2026

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Zweck und Geltungsbereich

Die Weisung erfasst KI-Dienste, eingebettete KI-Funktionen und automatisierte Entscheidungshilfen.

## Gilt für

- alle Mitarbeitenden, Organe und Beauftragten
- geschäftliche Nutzung auf Firmen- und Privatgeräten
- kostenlose und kostenpflichtige Dienste
- Beschaffung, Entwicklung, Pilotierung und Betrieb

## Sieben Governance-Grundsätze

- **Rechtmässigkeit**
- **Transparenz**
- **Fairness**
- **Rechenschaft**
- **Datenminimierung**
- **Menschliche Verantwortung**
- **Sicherheit**

**Die Weisung ergänzt Datenschutz-, Informationssicherheits-, Personal- und Fachweisungen. Strengere Vorgaben gehen vor.**

Rechtsgrundlagen: DSG Art. 6 und 8; OR Art. 328 und 328b; AI Act Art. 4.



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Zehn verbindliche Regeln für Mitarbeitende

Wer KI nutzt, bleibt für Eingaben, Prüfung und Verwendung des Outputs verantwortlich.

1. **Nur freigegebene Dienste und Firmenkonten nutzen**
2. **Keine geschützten Daten ohne ausdrückliche Freigabe eingeben**
3. **Daten minimieren und Identitäten wenn möglich ersetzen**
4. **Fakten, Quellen, Zahlen, Recht und Code prüfen**
5. **Wesentliche Entscheide nicht an KI delegieren**
6. **Relevanten KI-Einsatz dokumentieren und offenlegen**
7. **Urheber-, Persönlichkeits- und Nutzungsrechte beachten**
8. **Keine Schutzmechanismen oder Berechtigungen umgehen**
9. **Auffällige, falsche oder diskriminierende Ergebnisse melden**
10. **Bei Unsicherheit Nutzung stoppen und Fachstelle fragen**

**Zugangsdaten, Passwörter, private Schlüssel und vergleichbare Sicherheitsinformationen dürfen nie in KI-Systeme eingegeben werden.**

Grundlagen: DSG Art. 6, 8 und 19; vertragliche Geheimhaltung; URG; unternehmensinterne Informationsklassifikation.



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Risikoklassen steuern die Freigabe

Je grösser die Wirkung auf Personen, Rechte, Sicherheit oder Vermögen, desto höher die Kontrolltiefe.

## Niedrig

Öffentliche Inhalte, Sprachkorrektur, unverbindliche Ideensammlung.

Generelle Dienstfreigabe und Plausibilitätsprüfung.

## Mittel

Interne Entwürfe und Analysen ohne sensible Daten.

Fachverantwortung, Dokumentation und Stichproben.

## Hoch

Personendaten, HR, Kundenentscheide, Profiling sowie Rechts- und Sicherheitsprozesse.

Formelle Vorabfreigabe, Tests, Monitoring und menschliche Aufsicht.

## Unzulässig

Manipulation, rechtswidrige Überwachung, autonome wesentliche Entscheide oder Eingabe von Zugangsdaten.

Nutzung unterlassen und melden.

**Freigabekette bei hohem Risiko: Fachbereich → IT-Sicherheit → Datenschutz / Compliance → zuständiges Genehmigungsgremium**

Grundlagen: DSG Art. 22 (Datenschutz-Folgenabschätzung); AI Act Art. 6 und Anhang III.



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Für HR gelten erhöhte Anforderungen

KI kann vorbereiten und unterstützen. Personalentscheide verlangen eine eigenständige menschliche Beurteilung.

## Menschliche Letztentscheidung

Einstellung, Ablehnung, Leistungsbeurteilung, Beförderung, Vergütung, Versetzung, Disziplinarmassnahmen und Kündigung.

**KI-Output ist ein Input, kein Entscheid.**

- **Vorabfreigabe** — HR, Datenschutz / Compliance und IT-Sicherheit prüfen neue Anwendungen.
- **Transparenz** — Bewerbende und Mitarbeitende werden angemessen informiert.
- **Fairness** — Daten, Kriterien und Ergebnisse werden auf Verzerrungen geprüft.
- **Rechte** — Auskunft, Berichtigung, Anhörung und menschliche Überprüfung bleiben gewährleistet.
- **EU-Bezug** — Anwendbarkeit und mögliche Hochrisiko-Einstufung nach AI Act separat beurteilen.

Quellen: DSG Art. 19, 21, 22 und 25; OR Art. 328b; AI Act Art. 6, 26 und Anhang III Ziff. 4.



FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Governance über den gesamten Lebenszyklus

Freigabe allein genügt nicht. Anwendungen werden erfasst, überwacht, geändert und geordnet ausser Betrieb genommen.

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| **Bedarf** | **Prüfung** | **Test** | **Freigabe** | **Betrieb** | **Exit** |
| Zweck und Nutzen | Risiko, Recht und Anbieter | Qualität, Bias und Sicherheit | Rollen und Kontrollen | Monitoring und Vorfälle | Export und Löschung |

**Anbieterprüfung** — **Datenstandorte und Unterauftragnehmer · Training mit Eingaben · Zugriffsschutz und Protokolle · Rechte an Input und Output · Audit, Exit und Löschung**

Grundlagen: DSG Art. 8 und 9 sowie DSV; AI Act Art. 8–15 und 26, soweit anwendbar.

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Klare Rollen und ein schneller Meldeweg

Governance funktioniert nur, wenn Freigabe, Betrieb, Kontrolle und Eskalation eindeutig zugewiesen sind.

### Geschäftsleitung

Risikoappetit und wesentliche Freigaben

### KI-Verantwortliche Stelle

Inventar, Standards und Koordination

### Fachbereich

Zweck, Qualität und menschliche Aufsicht

### IT / Security

Technik, Zugriffe und Betriebsrisiken

### Datenschutz / Compliance

Recht, DSFA, Verträge und Transparenz

### Mitarbeitende

Sorgfalt, Prüfung, Dokumentation und Meldung

**Vorfälle sofort melden an [SERVICE DESK / SECURITY / DATENSCHUTZ]**

**Nutzung stoppen, Beweise sichern und keine eigenständige externe Kommunikation auslösen.**

Grundlagen: DSG Art. 24 (Meldung von Verletzungen der Datensicherheit); interne Incident- und Eskalationsprozesse.

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

# Umsetzung in vier Schritten

Vor Inkraftsetzung sind Verantwortlichkeiten, Dienste und Freigabewege konkret festzulegen.

| | | |
|---|---|---|
| 01 | **Verantwortung** | KI-Verantwortliche Stelle, Datenschutzkontakt und Genehmigungsgremium benennen. |
| 02 | **Bestand** | KI-Dienste und laufende Anwendungsfälle erfassen und risikoklassieren. |
| 03 | **Kontrollen** | Freigegebene Dienste, Datenregeln, Freigabeformular und Meldeweg veröffentlichen. |
| 04 | **Befähigung** | Mitarbeitende schulen und Hochrisiko-Anwendungen regelmässig überprüfen. |

**Vor Genehmigung zu ergänzen: Unternehmensname, Rollen, freigegebene Dienste, Kontaktstellen, Inkrafttreten und Prüfzyklus.**

Rechtsquellen und vollständige Handlungsvorgaben sind in der Word-Fassung der KI-Weisung enthalten.

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

INTERNE WEISUNG

# Weisung zum verantwortungsvollen Einsatz künstlicher Intelligenz

Erstentwurf für ein Schweizer KMU

| | |
|---|---|
| **Unternehmen** | [UNTERNEHMEN] |
| **Dokumenteigner** | [FUNKTION, z. B. Geschäftsleitung / Compliance] |
| **Genehmigt durch** | [GESCHÄFTSLEITUNG] |
| **Version / Status** | 0.1 / Entwurf |
| **Inkrafttreten** | [DATUM] |
| **Nächste Überprüfung** | [DATUM, spätestens nach 12 Monaten] |

**Zweck der Weisung**

Diese Weisung ermöglicht einen nutzbringenden Einsatz von KI und begrenzt rechtliche, sicherheitsbezogene und ethische Risiken. Sie verbindet Eigenverantwortung der Mitarbeitenden mit klaren Freigaben und wirksamer menschlicher Kontrolle.

*Rechtsstand: 16. September 2026*

## 1. Zweck, Geltungsbereich und Verbindlichkeit

Diese Weisung regelt die Auswahl, Beschaffung, Entwicklung und Nutzung von KI-Systemen bei [UNTERNEHMEN]. Sie gilt für alle Mitarbeitenden, Organe, temporär Beschäftigten und externen Personen, die im Auftrag des Unternehmens arbeiten. Sie erfasst sowohl eigenständige KI-Dienste als auch KI-Funktionen in Standardsoftware, Cloud-Diensten, Suchmaschinen, Kommunikations- und Fachanwendungen.

Die Weisung gilt unabhängig davon, ob ein Dienst kostenlos oder kostenpflichtig genutzt wird und ob der Zugriff

FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch