Informationsmaterial | SocialAI

KI in der Sozialen Arbeit

DSGVO und KI-VO

Dr. Heidi Scheichenbauer
Dr. Madeleine Müller, BA, MU

Wien, Oktober 2026

Research Institute – Digital Human Rights Center

Grundlage und Hinweis

Dieses Dokument bereitet die Inhalte des Innovationsworkshops Recht im Rahmen des Projekts Social AI[1], WP3, abgehalten am 30.06.2026 vom Research Institute – Digital Human Rights Center an der Uni Graz, für die Praxis der Sozialen Arbeit auf.
Es dient der Information und ersetzt keine Rechtsberatung im Einzelfall. Rechtsstand und Auslegungsfragen entsprechen dem Stand Oktober 2026.

[1] Das Projekt *SocialAI: Chancengerechtigkeit und KI in der Sozialen Arbeit* wird aus Mitteln der Nationalstiftung für Forschung, Technologie und Entwicklung (NATS) finanziert. Die Abwicklung des Förderungsprogramms Laura Bassi erfolgt durch die Österreichische Forschungsförderungsgesellschaft (FFG) und mit freundlicher mit Unterstützung des Bundesministeriums für Wirtschaft und Arbeit (BMAW). Das Projekt *SocialAI* wird an der Universität Graz (Projektleitung) in Kooperation mit Digital Humanities Craft OG; Jugend am Werk Steiermark GmbH, Research Institute AG & Co KG, SOS-Kinderdorf von 2026 - 2029 durchgeführt.

IMPRESSUM

Medieninhaberin und Herausgeberin:
Research Institute AG & Co KG
FB-Nr.: 355966f, HG Wien
Amundsenstraße 9, 1170 Wien

Das *Research Institute (RI) – Digital Human Rights Center* ist eine unabhängige Forschungseinrichtung an der Schnittstelle von Technik, Recht und Gesellschaft. Die Tätigkeiten des Institutes umfassen wissenschaftliche Forschung sowie Lehre und Consulting.

Web: https://researchinstitute.at
E-Mail: office@researchinstitute.at
Mastodon: mastodon.researchinstitute.at/@researchinstitute
© 2026 RI – Alle Rechte vorbehalten

HINWEIS zu gendergerechter Sprache

Die relevanten Gesetzestexte verwenden für die Beschreibung natürlicher und juristischer Personen das generische Maskulinum. Handelt es sich bei einem Begriff eindeutig um keine natürliche Person (zB Krankenhausträger, Bauträger), wird an der männlichen Form festgehalten. Auch Bezeichnungen, die aus dem Englischen entlehnt sind, bleiben in ihrer ursprünglichen Form erhalten (zB User, Provider). In allen anderen Fällen wird im Sinne eines diskriminierungsfreien Sprachgebrauchs das Gendersternchen verwendet.

Inhaltsverzeichnis

Auf einen Blick ... 1

1. Ausgangslage ... 2

1.1 Potenziale und Gefahren von KI ... 2

1.2 Der EU-Rechtsrahmen für KI ... 2

2. Die DSGVO in der Sozialen Arbeit ... 4

2.1. Grundlagen ... 4

Ursprünge ... 4

2.2. Was sind personenbezogene Daten? ... 5

Arten personenbezogener Daten ... 5

Bezug zur Praxis der Sozialen Arbeit ... 6

Berufliche Kontakte und juristische Personen ... 6

2.3. Verarbeitung und Anwendungsbereich ... 6

2.4. Rechtsgrundlagen ... 7

2.5. Wer ist wer? Rollen nach der DSGVO ... 7

Pflichten des Verantwortlichen und des Auftragsverarbeiters ... 8

3. KI-Verordnung (KI-VO) ... 9

3.1. Ziele und Ansatz ... 9

3.2. Anwendungsbereich und Begriff „KI-System“ ... 9

3.3. Wer ist wer? Rollen in der KI-VO ... 11

3.4. Der risikobasierte Ansatz ... 12

Verbotene Praktiken (Art 5) ... 12

Hochrisiko-KI (Art 6) ... 13

KI-Systeme mit Transparenzrisiko ... 14

KI-Systeme mit minimalem Risiko ... 15

General Purpose AI: Modell und System ... 15

3.5. KI-Kompetenz (Art 4) ... 16

3.6. Zusammenfassung Pflichten nach der KI-VO ... 16

3.7. Governance, Sanktionen und Haftung ... 17

4. DSGVO und KI-VO: Zusammenspiel ... 19

5. Mögliche Anwendungsfelder von KI in der Sozialen Arbeit ... 20

5.1. Anwendungsfall Fallarbeit ... 20

Vulnerabilität bei der Risikoeinschätzung ... 20

Datenschutz-Folgenabschätzung (DSFA) ... 21

Grundrechte-Folgenabschätzung (GRFA) ... 22

Automatisierte Einzelentscheidungen (Art 22 DSGVO) ... 23

5.2. Anwendungsfall Berichtswesen und Administration ... 25
Agentische KI ... 25
Rollenabgrenzung und Drittlandthematik ... 25
5.3. Anwendungsfall Contenterstellung ... 26
Transparenz- und Kennzeichnungspflichten (Art 50 KI-VO) ... 26
Urheberrecht im KI-Zeitalter ... 27
5.4. Anwendungsfall Chatbots im Beratungskontext ... 28
Kennzeichnung der Chatbot-Interaktion (Art 50 Abs 1 KI-VO) ... 28
KI-Haftung ... 29
Halluzinationen und Automation Bias ... 29
Offene Rechtsfrage ... 30
5.5. Exkurs: Blackbox, Bias und Diskriminierung ... 31
6. Checkliste: Vor dem Einsatz von KI-Tools ... 33
Zweck und Nutzen ... 33
Dateninput und Datenweg ... 33
Einfluss auf Einschätzungen und Entscheidungen ... 33
Bias, Diskriminierung und Chancengerechtigkeit ... 34
Transparenz, Grenzen und offene Rechtsfragen ... 34
7. Glossar ... 35
8. Quellen ... 36
8.1. Rechtsgrundlagen und Judikatur im Überblick ... 36
8.2. Weiterführende Quellen ... 36

Auf einen Blick

Generative Künstliche Intelligenz (KI) in Form von Chatbots, Textassistenten, Bild- und Audiogeneratoren hält zunehmend Einzug in die Soziale Arbeit und kann unter anderem beim Verfassen von Berichten, in der Fallarbeit, in der Öffentlichkeitsarbeit und in der Beratung unterstützen. Zwei Regelwerke prägen den rechtlichen Rahmen besonders: die **Datenschutz-Grundverordnung (DSGVO)** und die **KI-Verordnung (KI-VO oder auch AI Act)**.

Zentrale Punkte:

1	Die DSGVO ist immer anwendbar, wenn **personenbezogene Daten** verarbeitet werden, was auch für KI-Tools gilt. Sie folgt dem Grundsatz, dass jede Verarbeitung personenbezogener Daten verboten ist, außer sie ist explizit erlaubt. Die DSGVO enthält hierfür sogenannte „Erlaubnistatbestände", also Rechtsgrundlagen, nach denen Datenverarbeitungen gestattet sind. Klient*innendaten (Gesundheit, Herkunft) sind oft besonders schutzwürdig und ihre Verarbeitung unterliegt strengen Anforderungen.
2	Die KI-VO ergänzt die DSGVO und reguliert **KI-Systeme nach ihrem Risiko**, unabhängig davon, ob personenbezogene Daten verarbeitet werden. Einrichtungen, die KI im Berufsalltag einsetzen, sind in der Regel „Betreiber".
3	**KI-Kompetenz** ist essenzielle Voraussetzung für den verantwortungsvollen Umgang mit KI und die Erfüllung rechtlicher Verpflichtungen (Art 4 KI-VO). Sie gilt für alle Anbieter und Betreiber, unabhängig von der Risikoklasse des KI-Systems. Wer mit KI arbeitet, muss sie sachkundig einsetzen und ihre Risiken kennen.
4	**Hochrisiko-KI** ist im Sozialbereich ein relevantes Thema. So kann KI zur Beurteilung des Anspruchs auf grundlegende öffentliche Unterstützungsleistungen Hochrisiko-KI sein (Anhang III Nr 5a KI-VO). Oftmals bestehen beim Einsatz von KI zur Erstellung von Inhalten (Bilder, Texte, Videos) auch bestimmte **Transparenzpflichten** (Art 50 KI-VO).
5	Die **menschliche Letztentscheidung** muss gewährleistet sein. Wer KI-Empfehlungen blind folgt (Automation Bias, Abschnitt 5.4.), riskiert Fehler, Diskriminierung und einen Verstoß gegen Art 22 DSGVO.
6	**Transparenz und Prüfpflicht** sind zentral. Klient*innen sind über den KI-Einsatz zu informieren, KI-Ergebnisse können fehlerhaft sein und sind deshalb kritisch zu prüfen, und die Haftung bleibt bei der Einrichtung.

1. Ausgangslage

1.1 Potenziale und Gefahren von KI

Der zunehmende Einsatz von KI besitzt großes Potenzial, um Prozesse effizienter zu gestalten und Fachkräfte bei ihrer Aufgabenerfüllung zu unterstützen. Allerdings kann er auch Gefahren mit sich bringen, die vor dem konkreten KI-Einsatz bedacht werden müssen. Darüber hinaus werden dadurch philosophische Fragen aufgeworfen, was uns als Menschen auszeichnet und worin unsere Aufgabe liegt.

Potenziale	Gefahren
• Produktivitäts- und Effizienzsteigerung, weniger administrative Aufgaben • Erweiterung von Fähigkeiten und Wissen; Zugang zu Information; Teilhabe • Innovationspotenzial, neue Lösungswege • Fortschritte in Medizin und Diagnostik, Optimierung kritischer Infrastruktur • Mehr Sicherheit in verschiedenen Sektoren	• Eingriffe in Privatsphäre und Persönlichkeitsrechte durch Überwachung • Verletzung von Grund- und Menschenrechten (Diskriminierung, Menschenwürde, Informationsfreiheit) • Schwierige Nachvollziehbarkeit („Black-Box-Problematik“) • „Deskilling“, „Automation Bias“, „Confirmation Bias“ • Kontextspezifische Herausforderungen (Arbeitsrecht, Bildung, Konsumentenschutz) • Arbeitsmarktverdrängung, Machtkonzentration, Entmenschlichung • Desinformation und Deepfakes

Aus diesem Grund bedarf es rechtlicher Schranken, um die Gefahren so gering wie möglich zu halten, während die Potenziale von KI ausgeschöpft werden können.

1.2 Der EU-Rechtsrahmen für KI

Es gibt nicht „das eine“ KI-Gesetz, das alle relevanten Aspekte dieser Technologie regelt. Die KI-VO stellt zwar die einzige horizontale (sektorübergreifende), rechtsverbindliche Regulierung von KI am europäischen Binnenmarkt dar, steht jedoch neben zahlreichen weiteren EU-Rechtsakten, die für KI-Anwendungen relevant sind:

Themenfeld	Wichtige Rechtsakte
Grundrechte	Datenschutz inklusive ausschließlich automatisierter Einzelentscheidungen, Diskriminierungsverbote, Arbeitnehmerrechte, Meinungsfreiheit
Datenverfügbarkeit	Data Governance Act, Data Act
Cyber- und Produktsicherheit	NIS2, weitere Cybersecurity-Rechtsakte, Produktsicherheitsverordnungen
Wettbewerb, Konsumentenschutz, Copyright	Gesetz über digitale Dienste (unter anderem algorithmische Inhaltsmoderation, Risikomanagement, Grundrechtsschutz), Gesetz über digitale Märkte
Haftungsrecht	Novellierte Produkthaftungsrichtlinie (PHRL)

Auf **europäischer Ebene** ging der Regulierung ein längerer Prozess voraus (Erklärungen, ethische Leitlinien für vertrauenswürdige KI, Weißbuch). Parallel wurde das **Rahmenübereinkommen des Europarats** über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit verhandelt und am 5. September 2024 unter anderem von EU, UK und USA unterzeichnet – der erste rechtsverbindliche internationale Vertrag, der einen Standard für vertrauenswürdige KI setzen soll.

2. Die DSGVO in der Sozialen Arbeit

2.1. Grundlagen

Sobald mittels KI personenbezogene Daten verarbeitet werden, ist die DSGVO zu beachten. Zu schützen sind nicht die Daten selbst, sondern **die Menschen, über die Daten verarbeitet werden**. Datenschutz ist Voraussetzung für das Funktionieren einer freien demokratischen Gesellschaft und für die Ausübung zahlreicher anderer Grundrechte. Es geht also nicht primär um den Schutz von Daten vor Zerstörung oder Diebstahl, sondern um das Grundrecht auf Privatsphäre in der Informationsgesellschaft.

- Die DSGVO enthält Vorschriften zum **Schutz natürlicher Personen**[2] bei der Verarbeitung personenbezogener Daten **und zum freien Verkehr** solcher Daten.
- Datenschutz gilt **nicht absolut**, sondern ist einer Abwägung zugänglich: Andere Grundrechte und Interessen (Meinungs- und Informationsfreiheit, Eigentum, öffentliche Interessen) können das Recht auf Datenschutz einschränken.

Ursprünge

Das Recht auf Privatleben:	• Art 8 Abs 1 Europäische Menschenrechtskonvention (1950): „Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.“
Das Recht auf Schutz der personenbezogenen Daten:	• Art 16 Abs 1 AEUV und Art 8 EU-Grundrechte-Charta: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“ (eigenes Grundrecht auf Datenschutz)

Ziele und Auswirkungen der DSGVO sind die Stärkung der Betroffenenrechte, mehr Eigenverantwortung der Datenverarbeiter, größere Harmonisierung in Europa, erweiterter Anwendungsbereich durch das Marktortprinzip (auch Nicht-EU-Anbieter, die in der EU anbieten, zB Facebook, Google, Amazon), höhere Strafdrohungen und die Möglichkeit von Schadenersatzklagen.

[2] Der Begriff „natürliche Person“ ist ein juristischer Fachbegriff und bezieht sich auf Menschen im Unterschied zu Gesellschaften, Vereinen und Unternehmen, die gemeinhin als „juristische Personen“ bezeichnet werden.

2.2. Was sind personenbezogene Daten?

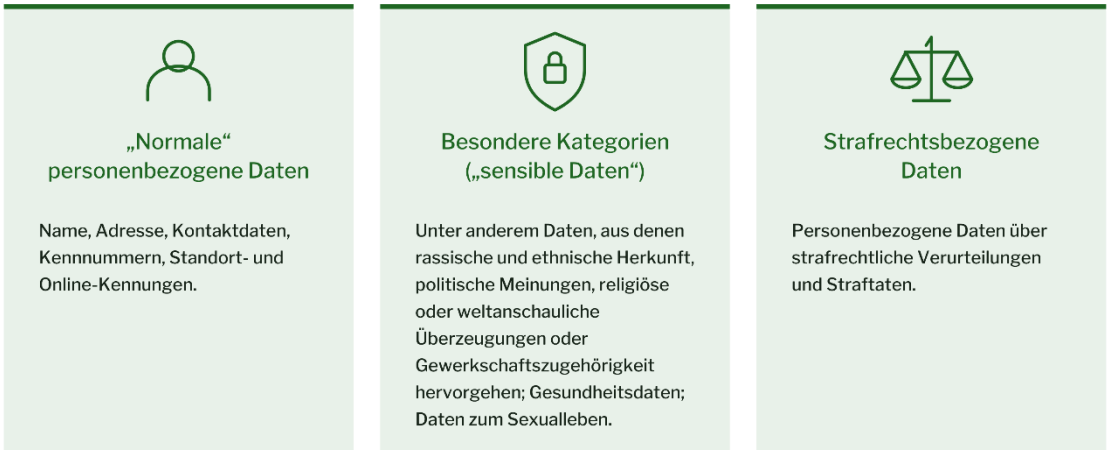
Personenbezogene Daten sind **alle Informationen, die sich auf eine identifizierte oder identifizierbare (lebende) natürliche Person beziehen**.[3] Identifizierbar ist eine Person, die direkt oder indirekt – insbesondere mittels Zuordnung zu einer Kennung wie Name, Kennnummer, Standortdaten oder Online-Kennung – identifiziert werden kann.

- Der Begriff „alle Informationen" ist **weit** zu verstehen und nicht auf sensible oder vertrauliche Informationen beschränkt.
- Erfasst sind **objektive wie subjektive Informationen** (Stellungnahmen, Beurteilungen), sofern sie Informationen „über" die Person darstellen.

> **Beispiele aus der Sozialen Arbeit:**
> Für die Soziale Arbeit heißt das: Auch Einschätzungen, Gesprächsnotizen und Risikobewertungen zu Klient*innen sind personenbezogene Daten.

- **Identifizierbarkeit**: Zu berücksichtigen sind „alle Mittel, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden", um eine bestimmte Person zu identifizieren.[4]

Arten personenbezogener Daten



[3] Siehe die Definition in Art 4 Z 1 DSGVO.
[4] Siehe ErwGr 26 DSGVO.

Bezug zur Praxis der Sozialen Arbeit

Klient*innenakten in der Sozialen Arbeit enthalten häufig Gesundheitsdaten, Angaben zu Herkunft, Familie, Gewalterfahrungen oder Straftaten. Beim Einsatz von KI-Tools ist daher regelmäßig von sensiblen Daten oder von strafrechtsbezogenen Daten auszugehen – mit strengeren Anforderungen.

Berufliche Kontakte und juristische Personen

- Nach DSGVO besteht **kein Schutz für juristische Personen** (zB Vereine, Unternehmen). Name, Rechtsform oder Kontaktdaten der juristischen Person (zB Office-Adresse) sind in der Regel nicht geschützt.
- Österreichische Besonderheit: Die **Verfassungsbestimmung des § 1 DSG („Recht auf Geheimhaltung für jedermann")** gilt auch für juristische Personen. Nach der Entscheidungspraxis der österreichischen Datenschutzbehörde (DSB) können sich diese in nationalen Fällen auf Rechte wie Auskunft, Richtigstellung und Löschung berufen.
- Datenschutz gilt weiterhin uneingeschränkt für natürliche Personen, die für juristische Personen arbeiten.

2.3. Verarbeitung und Anwendungsbereich

Um der DSGVO zu unterliegen, muss eine **Verarbeitung** personenbezogener Daten stattfinden. Der Verarbeitungsbegriff ist umfassend: Er reicht von der Erhebung, Erfassung und Organisation über Ordnen und Speichern, die Anpassung, Veränderung, das Auslesen, Abfragen, die Verwendung, Offenlegung und Übermittlung bis zu Verbreitung, Abgleich, Verknüpfung, Einschränkung, Löschung oder Vernichtung von Daten.

Beachte: Schon das Eintippen von Fallinformationen (zB Name, Geburtsdatum, Hintergrund, Familienverhältnisse) in ein KI-Tool ist in der Sozialen Arbeit eine Verarbeitung.

Die DSGVO **gilt** für …	Die DSGVO **gilt nicht** für …
• ganz oder teilweise elektronische Verarbeitung personenbezogener Daten • Verarbeitung in Papierform, sofern die Daten nach bestimmten Kriterien geordnet sind	• unstrukturierte Verarbeitung in Papierform (es gilt jedoch das Recht auf Geheimhaltung nach § 1 DSG; keine DSGVO-Strafen) • Tätigkeiten natürlicher Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten

2.4. Rechtsgrundlagen

Personenbezogene Daten **dürfen nur verarbeitet werden**, wenn die Verarbeitung auf eine der in Art 6 DSGVO genannten Rechtsgrundlagen gestützt werden kann. Dazu zählen unter anderem die Einwilligung der betroffenen Person, die Notwendigkeit der Verarbeitung für die Erfüllung eines Vertragsverhältnisses (zB die Verarbeitung von Beschäftigtendaten zur Erfüllung des Dienstvertrags) und das „berechtigte Interesse" (wenn eine Einrichtung darlegen kann, dass ihr Interesse an der Datenverarbeitung das Interesse der betroffenen Person an der Geheimhaltung ihrer Daten überwiegt).

Für die Verarbeitung **sensibler Daten und strafrechtsbezogener Daten** gelten zusätzliche, **strengere Anforderungen**.[5]

2.5. Wer ist wer? Rollen nach der DSGVO

Rolle	Bedeutung und Beispiele
Verantwortlicher *(Art 4 Z 7 DSGVO)*	Natürliche oder juristische Person, die über Mittel und Zwecke der Verarbeitung entscheidet – also das „Wie" und „Wozu" der Datenverarbeitung. In der Regel ist das die Organisation, also der Rechtsträger bzw die Einrichtung (NPO).
Auftragsverarbeiter *(Art 4 Z 8 iVm Art 28 DSGVO)*	Person oder Einrichtung, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, zB IT-Dienstleister, Provider sowie KI-Anbieter. Erforderlich ist hier eine Auftragsverarbeitervereinbarung zwischen Verantwortlichem und Auftragsverarbeiter, in der die Bedingungen der Zusammenarbeit geregelt sind (zB der Gegenstand und die Dauer der Datenverarbeitung, der Zweck und die Datenkategorien).
Mitarbeitende	Am häufigsten sind Mitarbeitende Betroffene (wenn der Arbeitgeber ihre Daten verarbeitet). Verarbeiten sie im Rahmen ihrer Tätigkeit Daten, handeln sie auf Weisung des Arbeitgebers und sind keine eigenständige Akteure. Nur bei eigenmächtiger Verarbeitung außerhalb beruflicher Pflichten (zB private Nutzung, „Mitarbeiterexzess") werden sie selbst Verantwortliche.

Achtung: Private Tools vermeiden

Nutzt eine Fachkraft ein privates KI-Konto und gibt dort Fallinformationen ein, fehlt in der Regel jede rechtliche Grundlage. Man spricht hier auch von sogenannter „Schatten-KI", also der unautorisierten oder unkontrollierten KI-Nutzung durch Beschäftigte ohne Wissen oder Freigabe

[5] Siehe die dazu notwendigen Voraussetzungen in Art 9 Abs 2 DSGVO im Fall von sensiblen Daten und Art 10 DSGVO in Bezug auf strafrechtsbezogene Daten.

des Arbeitgebers. Der Träger sollte daher klar regeln, welche Tools genehmigt sind, beispielsweise in einer internen KI-Richtlinie.
Außerdem erhält man eine Auftragsverarbeitervereinbarung meist nur bei kostenpflichtigen Diensten. Auch muss beachtet werden, ob Drittlandtransfers – also die Übermittlung von Daten in Länder außerhalb der EU – erfolgen und ob diese zulässig sind.

Pflichten des Verantwortlichen und des Auftragsverarbeiters

Pflicht	Wen betrifft sie?
Rechenschaftspflicht bezüglich der Einhaltung der DSGVO	Verantwortlicher
Betroffenenrechte und Informationspflichten	Verantwortlicher (Unterstützung durch Auftragsverarbeiter)
Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	Verantwortlicher
Verzeichnis von Verarbeitungstätigkeiten	Verantwortlicher und Auftragsverarbeiter
Meldung von Datenschutzverletzungen	Verantwortlicher (Unterstützung durch Auftragsverarbeiter)
Datenschutz-Folgenabschätzung	Verantwortlicher (Unterstützung durch Auftragsverarbeiter)
Verpflichtender Datenschutzbeauftragter	kann Verantwortlichen und/oder Auftragsverarbeiter betreffen
Datensicherheitsmaßnahmen	Verantwortlicher und Auftragsverarbeiter
Prüfung, ob der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zur Einhaltung der DSGVO gesetzt hat, bevor dieser beauftragt wird	Verantwortlicher
Datenverarbeitung nur auf Weisung des Verantwortlichen; Löschung/Rückgabe der Daten nach Auftragsbeendigung und Übermittlung aller erforderlichen Informationen	Auftragsverarbeiter

3. KI-Verordnung (KI-VO)

3.1. Ziele und Ansatz

Die **Verordnung (EU) 2024/1689** („KI-Verordnung", „KI-VO" oder „AI Act") legt harmonisierte Vorschriften für künstliche Intelligenz fest.

- **Horizontaler Regulierungsansatz** für das Inverkehrbringen und den Betrieb bestimmter KI-Systeme. Dies bedeutet, dass die KI-VO sektorunabhängig gilt.
- **Duale Zielsetzung:** Regulierung von Risiken und hohes Schutzniveau für Grundrechte (zB Nichtdiskriminierung) einerseits, Förderung von Innovation andererseits.
- **Ansatz Produktsicherheit**: KI wird als Produkt verstanden, das gewissen Mindestanforderungen unterliegen muss. Dazu dient beispielsweise die Konformitätsbewertung, mit der die Einhaltung der entsprechenden Vorschriften bescheinigt wird, wobei dies durch technische Normen und Standards konkretisiert sowie durch Marktüberwachung sichergestellt wird.
- **Ausnahmen, wann die KI-VO nicht gilt:** nicht unter Unionsrecht fallende Bereiche (zB Militär), Forschungsausnahmen, Systeme unter quelloffenen Lizenzen, persönlicher Gebrauch.

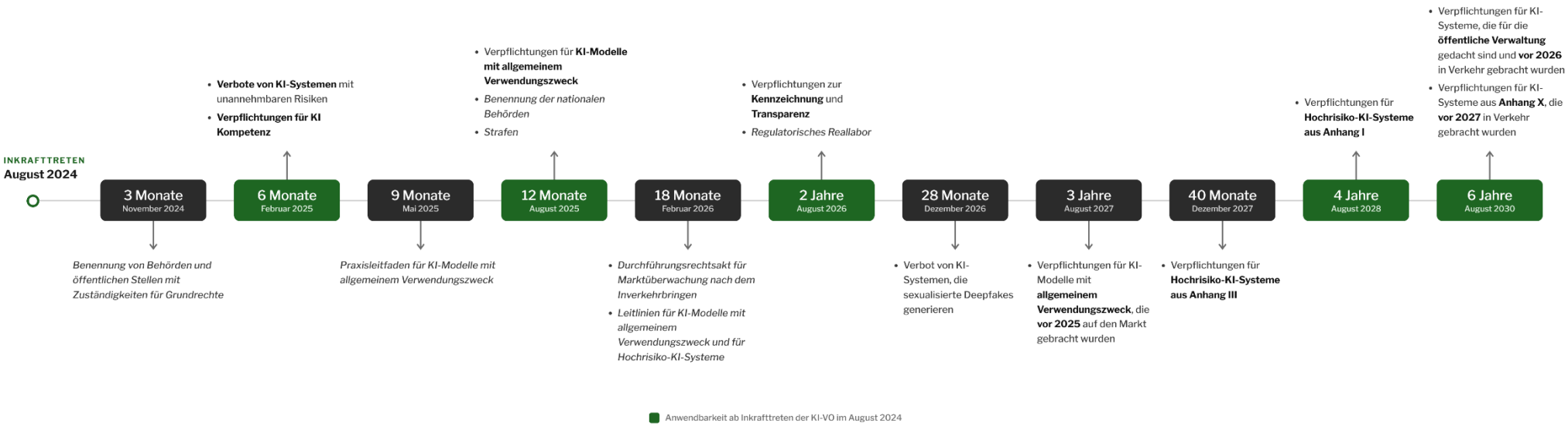
3.2. Anwendungsbereich und Begriff „KI-System"

Sachlich	Die KI-VO gilt für KI-Systeme oder KI-Modelle mit allgemeinem Verwendungszweck („General Purpose AI", GPAI)
Räumlich	KI-Systeme, die in der EU in Verkehr gebracht oder in Betrieb genommen werden oder deren hervorgebrachte Ausgabe in der EU verwendet wird
Zeitlich	Die KI-VO wird gestaffelt anwendbar, dh ihre Bestimmungen erlangen abgestuft innerhalb von 6-48 Monaten nach ihrem Inkrafttreten Geltung (siehe Abbildung sogleich)[6]

[6] Hinweis: Die konkreten Anwendungsfristen einzelner Bestimmungen wurden durch ein Gesetzespaket („Digitaler Omnibus zur KI") verschoben und sind hier in ihrer aktuellen Fassung dargestellt (Verordnung (EU) 2026/1744 des Europäischen Parlaments und des Rates vom 8. Juli 2026 zur Änderung der Verordnungen (EU) 2024/1689, (EU) 2018/1139 und (EU) 2023/1230 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), ABl L 2026/1744, 24.7.2026).

KI-VO

Zeitplan ab Inkrafttreten (August 2024)



Definition „KI-System“ (Art 3 Z 1 KI-VO):

Ein KI-System ist ein **maschinengestütztes** System, das für einen in unterschiedlichem Grade **autonomen Betrieb** ausgelegt ist, nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und aus den erhaltenen **Eingaben** für explizite oder implizite Ziele **ableitet**, wie **Ausgaben** (Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen) hervorgebracht werden, die physische oder virtuelle **Umgebungen** beeinflussen können.

Ziel ist die Abgrenzung zu herkömmlicher Software, die lediglich auf vordefinierten, menschlichen Regeln beruht. KI wiederum basiert oft auf Methoden des maschinellen Lernens und umfasst logik- und wissensgestützte Systeme. Die Kommission hat dazu **Leitlinien**[7] veröffentlicht und Beispiele von Systemen genannt, die *nicht* unter den KI-Begriff fallen (zB logistische Regression, einfache Datenverarbeitung).

- **Beispiele für KI:** Chatbots wie ChatGPT, Claude, Copilot Chat, Gemini etc., da diesen in der Regel große Sprachmodelle zugrunde liegen, die auf Methoden des maschinellen Lernens basieren.
- **Keine KI:** Einfache „Wenn-Dann“-Algorithmen, Verwaltung einer Excel-Liste, grundlegende Datenverarbeitung, herkömmliche Softwarelösungen.

3.3. Wer ist wer? Rollen in der KI-VO

Die Anforderungen bzw einzuhaltenden Verpflichtungen variieren einerseits je nach der Rolle einer Einrichtung nach der KI-VO:

Rolle	Definition
Anbieter *(Art 3 Z 3 KI-VO)*	Person oder Stelle, die ein KI-System oder GPAI-Modell entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder in Betrieb nimmt, sei es entgeltlich oder unentgeltlich. Fällt oft mit dem Hersteller des Systems zusammen.
Betreiber *(Art 3 Z 4 KI-VO)*	Person oder Stelle, die ein KI-System in eigener Verantwortung im Rahmen ihrer beruflichen Tätigkeit verwendet.

Die KI-VO kennt weitere Rollen (Bevollmächtigter, Einführer, Händler). Träger der Sozialen Arbeit, die ein am Markt erhältliches Tool unverändert einsetzen, fungieren in der Regel als **Betreiber**.

Achtung: Wer ein KI-System wesentlich verändert oder unter eigenem Namen anbietet, kann unter bestimmten Voraussetzungen selbst zum Anbieter werden (sogenannte **Anbieterfiktion** nach Art 25 KI-VO).

[7] https://ec.europa.eu/newsroom/dae/redirection/document/118628.

3.4. Der risikobasierte Ansatz

Weiters bestimmen sich die Pflichten nach der **Risikoeinstufung** eines KI-Systems. Denn die KI-VO ordnet KI-Systeme vier Risikostufen zu und folgt dabei dem Grundsatz: Je höher das Risiko, desto strenger die Pflichten. Das Risiko kann dabei entweder vom KI-Produkt selbst ausgehen oder sich durch dessen Einsatzbereich ergeben. Maßgeblich für die Risikoeinstufung ist der konkrete **Verwendungszweck**.

Risikostufe	Typische Merkmale	Rechtsfolge
Unannehmbares Risiko	Verstoß gegen die Grundrechte und Werte der Union	Verbot (Art 5)
Hohes Risiko	Auswirkungen auf Gesundheit, Sicherheit oder Grundrechte	Konformitätsbewertung, Überwachung nach dem Inverkehrbringen, breiter Pflichtenkatalog für Anbieter und Betreiber (Art 6-49)
Transparenzrisiko	Risiko von Imitation, Manipulation oder Täuschung (zB Chatbots, Deepfakes, KI-generierte Inhalte)	Informations- und Transparenzpflichten (Art 50)
Minimales Risiko	Sonstige KI-Systeme	Unterstützung der Belegschaft beim Aufbau von KI-Kompetenz (Art 4); freiwillige Verhaltenskodizes (Art 95)

Anbieter von GPAI-Modellen (Modelle mit allgemeinem Verwendungszweck) unterliegen eigenen Pflichten. Anbieter von GPAI-Modellen mit **systemischem Risiko** haben zusätzliche Pflichten zur Risikobewertung und -minderung zu beachten.

Verbotene Praktiken (Art 5)

- **Manipulative KI-Systeme** (zB Algorithmen, die Personen unbewusst zu Kaufentscheidungen drängen)
- KI-Systeme, die **Vulnerabilitäten ausnutzen** (zB Alter, Behinderung, soziale Situation)
- **Sexualisierte Deepfakes** und **kinderpornographisches** Material
- **Sozialkreditsysteme** (Bewertung und Benachteiligung aufgrund des sozialen Verhaltens)
- **„Predictive Policing“** (Vorhersage von kriminellem Verhalten aufgrund von Charaktereigenschaften)
- Ungezieltes Auslesen von Datenbanken zur Gesichtserkennung **(„Scraping“)**
- **Emotionserkennungs-KI** am Arbeitsplatz und im Bildungsbereich



- **Biometrische Kategorisierungssysteme** (Ableitung „sensibler“ Eigenschaften aus biometrischen Daten)
- **Echtzeit-Biometrie** in öffentlichen Räumen (mit Ausnahmen)

Beachte:

Das Ausnutzen von Vulnerabilitäten berührt den Kern der Klient*innenarbeit. Systeme, die Alter, Behinderung oder soziale Lage von Klient*innen gezielt ausnutzen oder Personen nach ihrem sozialen Verhalten bewerten, wären unzulässig.

Hochrisiko-KI (Art 6)

Es gibt zwei Wege zur Einstufung als Hochrisiko-KI:

- **„Eingebettete“ Hochrisiko-KI-Systeme (Art 6 Abs 1):** KI als Sicherheitskomponente eines Produkts oder selbst als Produkt, das unter die Harmonisierungsrechtsvorschriften des Anhangs I fällt und einer Konformitätsbewertung durch Dritte unterliegt, zB Medizinprodukte oder Spielzeug.
- **„Eigenständige“ Hochrisiko-KI-Systeme (Art 6 Abs 2):** in **Anhang III** genannte Bereiche:
  - Erlaubte Biometrie und Emotionserkennung
  - Sicherheitsbauteile in der kritischen Infrastruktur (Wasser-, Strom-, Gasversorgung),
  - Bildung und Zugang zum Bildungsbereich
  - Beschäftigung und Personalmanagement, insb in Bewerbungsverfahren und zur Leistungskontrolle bzw in Entscheidungsprozessen
  - Grundlegende (öffentliche und private) Leistungen (zB Gesundheitsleistungen, öffentliche Beihilfen, Prämien in Kranken- und Lebensversicherung, Bonitätsprüfung, Triage und Notrufreihung)
    Strafverfolgung,
  - Migration/Asyl/Grenzkontrolle
  - Justiz und Demokratie.

Ein in Anhang III genanntes KI-System gilt **ausnahmsweise nicht als hochriskant**, wenn es kein erhebliches Risiko der Beeinträchtigung von Gesundheit, Sicherheit oder Grundrechten birgt (**Ausnahme in Art 6 Abs 3**). Dies ist unter anderem der Fall, wenn es keinen wesentlichen Einfluss auf Entscheidungsfindungen hat, weil es nur vorbereitende Aufgaben durchführt, menschliche Tätigkeiten verbessert, eng gefasste Verfahrensaufgaben übernimmt oder Entscheidungsmuster erkennt. Ein Beispiel wären KI-Systeme, die zwar in Bewerbungsprozessen eingesetzt werden, die Bewerbungen allerdings nur indexieren, ohne der Einstellungsentscheidung vorzugreifen.

Wichtige Rückausnahme: Profiling

Nimmt ein Anhang-III-System **Profiling** natürlicher Personen vor, gilt es immer als hochriskant (auch wenn die oben genannte Ausnahme greifen würde). Profiling ist jede automatisierte Verarbeitung personenbezogener Daten, um persönliche Aspekte einer Person (zB Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Vorlieben, Zuverlässigkeit, Verhalten, Aufenthaltsort) zu bewerten, zu analysieren oder vorherzusagen.[8] Berichts- und Auswertungstools, die Klient*innen bewerten oder Prognosen erstellen, sind daher besonders sorgfältig zu prüfen.

KI-Systeme mit Transparenzrisiko

Art 50 KI-VO sieht für bestimmte Systeme Transparenzpflichten vor. **Anbieter** müssen Personen über die **Interaktion mit KI informieren**, sofern diese nicht offensichtlich ist. Dies ist beispielsweise einschlägig, wenn Klient*innen mit Chatbots einer sozialen Einrichtung kommunizieren und fälschlicherweise davon ausgehen könnten, mit einem*r Sachbearbeiter*in zu interagieren. Außerdem müssen Anbieter **künstlich erzeugte Inhalte maschinenlesbar** kennzeichnen, etwa durch Wasserzeichen oder Metadaten. **Betreiber** müssen die Verwendung von Systemen zur Biometrie und Emotionserkennung offenlegen sowie **Deepfakes** als KI-generiert **kennzeichnen**. Unter „Deepfakes" versteht man KI-generierte oder -manipulierte Bild-, Ton- oder Videoinhalte, die echten Personen, Einrichtungen, Orten oder Ereignissen ähneln und als echt erscheinen.[9] Ebenso müssen KI-generierte Texte, die zur Information der Öffentlichkeit über Angelegenheiten von öffentlichem Interesse veröffentlicht werden, gekennzeichnet werden, sofern keine menschliche Überprüfung oder redaktionelle Kontrolle erfolgt.

Die Kommission veröffentlichte im Juli 2026 **Leitlinien zu diesen Transparenzpflichten**.[10] Ein ergänzender **Verhaltenskodex** unterstützt Anbieter und Betreiber bei der rechtskonformen Kennzeichnung und kann freiwillig unterzeichnet werden.[11] Er enthält zudem öffentlich verfügbare Symbole, mit denen Betreiber KI-generierte Inhalte nach Art 50 Abs 4 KI-VO kennzeichnen können:

Icon	Verwendung	Beispiele
Basissymbol 	Wenn KI an der Erstellung von Deepfakes (Bild, Audio, Video) oder veröffentlichtem Text beteiligt war oder wenn ein benutzerdefiniertes Textlabel oder eine interaktive zweite Ebene implementiert sind.	Deepfake-Video mit dem Text „Stimmen generiert mit" gefolgt vom Basissymbol
Vollständig KI-generiert 	Wenn das Deepfake (Bild, Audio, Video) oder der Text vollständig von KI generiert wird, ohne von Menschen geschaffene Elemente oder menschliche redaktionelle Kontrolle (abgesehen von den KI-Eingaben bzw „Prompts").	Vollständig KI-generierte Deepfake-Videos mit Personen des öffentlichen Lebens Vollständig KI-komponierte Musik oder Kunst[12]

[8] (Art 3 Z 52 KI-VO iVm Art 4 Z 4 DSGVO).
[9] Die Definition von „Deepfakes" findet sich in Art 3 Z 60 KI-VO.
[10] https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems.
[11] https://digital-strategy.ec.europa.eu/de/policies/code-practice-ai-generated-content.
[12] Hier können begrenzte Offenlegungsanforderungen für künstlerische, fiktive oder satirische Werke gemäß Art 50 Abs 4 KI-VO bestehen.

		KI-generierte Nachrichtenzusammenfassungen
Teilweise KI-modifiziert 	Wenn bereits bestehende, von Menschen erstellte Inhalte teilweise modifiziert wurden, sodass diese zu einem Deepfake oder Text von öffentlichem Interesse werden.	Ein Gesicht in einem authentischen Foto wird mithilfe von KI mit dem Gesicht eines Politikers bzw einer Politikerin getauscht Authentische Fotos einer leeren Wohnung werden mit KI eingerichtet

KI-Systeme mit minimalem Risiko

Alle anderen KI-Systeme gelten als „minimal riskant". Die KI-VO kennt dafür kaum allgemeine Pflichten – die einzige Bestimmung, die Anforderungen an Anbieter und Betreiber gleichermaßen unabhängig von der Risikoeinstufung des KI-Systems stellt, ist Art 4 zur **KI-Kompetenz** (siehe unten in Abschnitt 3.5.). Es ist jedoch möglich, sich freiwilligen Verhaltenskodizes zu unterwerfen und die Verpflichtungen für Hochrisiko-KI einzuhalten (Art 95 KI-VO). Sonstige Verpflichtungen, wie etwa anderes Produktsicherheitsrecht, Cybersecurity-Vorschriften, Wettbewerbsrecht, Grund- und Menschenrechte, Datenschutzrecht und ethische Compliance, bleiben davon unberührt.

General Purpose AI: Modell und System

Ein KI-Modell stellt gewissermaßen den „Motor" hinter KI-Anwendungen dar und leistet die eigentliche Arbeit, wird jedoch erst über die Einbettung in eine Anwendungsumgebung mit Schnittstellen und Benutzeroberflächen („KI-System") einsetzbar. Dennoch knüpft die KI-VO rein an den Begriff des KI-Systems an und der Begriff des KI-Modells ist ihr grundsätzlich fremd. Die KI-VO enthält lediglich vereinzelte Verpflichtungen für Anbieter sogenannter „KI-Modelle mit allgemeinem Verwendungszweck" („General Purpose AI" oder „GPAI").

Ein **GPAI-Modell** ist ein KI-Modell mit erheblicher allgemeiner Verwendbarkeit, das ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen und in eine Vielzahl nachgelagerter Systeme integriert werden kann.[13] Ein **GPAI-System** ist ein KI-System, das auf einem solchen GPAI-Modell beruht und einer Vielzahl von Zwecken dienen kann.[14] Gängige Chatbots wie ChatGPT bauen auf GPAI-Modellen auf und sind selbst GPAI-Systeme. Sie sind wiederum nach den Risikoklassen der KI-VO einzustufen, wobei die Einstufung von ihrem konkreten Zweck abhängt.

Für GPAI-Modelle existiert seit 10. Juli 2025 ein **Praxisleitfaden** (General-Purpose AI Code of Practice) mit den Kapiteln Sicherheit, Urheberrecht und Transparenz, den unter anderem Amazon, Anthropic, Google, IBM, Microsoft, Mistral und OpenAI unterzeichnet haben.[15]

[13] Siehe die Definition in Art 3 Z 63 KI-VO.
[14] Siehe die Definition in Art 3 Z 66 KI-VO.
[15] https://digital-strategy.ec.europa.eu/de/policies/contents-code-gpai.

3.5. KI-Kompetenz (Art 4)

KI-Kompetenz (Art 3 Z 56) bezeichnet die Fähigkeiten, Kenntnisse und das Verständnis, KI-Systeme **sachkundig einzusetzen** sowie sich der **Chancen und Risiken von KI und möglicher Schäden** bewusst zu werden. Anbieter und Betreiber von KI-Systemen müssen Maßnahmen ergreifen, um die Entwicklung der KI-Kompetenz ihres Personals und anderer Personen, die mit KI operieren, zu unterstützen, damit diese über ein **ausreichendes Maß an KI-Kompetenz** verfügen. Zu berücksichtigen sind technische Kenntnisse, Erfahrung, Ausbildung, der Kontext und die betroffenen Personengruppen.

- Die Pflicht zur Maßnahmenergreifung gilt für alle Anbieter und Betreiber, unabhängig von der Risikoklasse.
- Fortbildung soll laufend, zielgruppenorientiert und methodisch vielfältig sein. Es existiert **kein „One-size-fits-all-Zugang"**.
- Sie umfasst rechtliche, technische, soziale und ethische Komponenten.
- Empfehlung: Entwicklung interner KI-Richtlinien und Ernennung einer bzw eines „KI-Beauftragten".
- Orientierung bietet das **„Living Repository"**[16] der EU-Kommission mit **Best-Practice-Beispielen** aus den Mitgliedstaaten.

Praxis-Tipp:
Dokumentieren Sie Schulungen und interne Regeln zum KI-Einsatz. Für Teams der Sozialen Arbeit bietet sich eine kurze Einführung mit fachspezifischen Beispielen (Fallnotizen, Berichte, Klient*innenkommunikation) an. Mögliche Maßnahmen sind externe Seminare, interne Workshops, E-Learning-Module oder „Peer-to-Peer-Learning".

3.6. Zusammenfassung Pflichten nach der KI-VO

Folgende Tabelle gibt eine Übersicht über die wesentlichen Verpflichtungen nach der KI-VO, geordnet nach relevantem Akteur (Anbieter oder Betreiber) und Risikokategorie.[17]

System und Rolle	Wesentliche Anforderungen
Anbieter von Hochrisiko-KI bzw allgemeine Anforderungen	Sie erfüllen Anforderungen an Risikomanagement, Datenqualität, Dokumentation, Protokollierung, Transparenz, menschliche Aufsicht, Genauigkeit, Robustheit und Cybersicherheit (Art 9 bis 15)

[16] https://digital-strategy.ec.europa.eu/en/policies/ai-literacy-practices.
[17] Für eine detaillierte Übersicht siehe: https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Anbieterverpflichtungen.de.html und https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Betreiberverpflichtungen.de.html. Vgl auch in abgewandelter Form: *Müller/Treitl,* Risikobasierter Ansatz, LexisNexis Glossar KI-VO (iE).

System und Rolle	Wesentliche Anforderungen
Anbieter von Hochrisiko-KI	Sie organisieren Qualitätsmanagement, Aufbewahrung, Korrekturen, Behördenkooperation, gegebenenfalls Bevollmächtigung und Registrierung sowie Konformitätsbewertung, -erklärung und CE-Kennzeichnung (Art 16 bis 22 und 43 bis 49)
Betreiber von Hochrisiko-KI	Sie verwenden das System nach Anleitung, gewährleisten kompetente menschliche Aufsicht, kontrollieren relevante Eingabedaten und überwachen den Betrieb. Sie bewahren verfügbare Protokolle mindestens 6 Monate auf. Ebenso erfüllen sie einschlägige Informationspflichten (Art 26). Unter gewissen Voraussetzungen können Betroffene ein Recht auf Erläuterung gegen sie geltend machen (Art 86).
Bestimmte Betreiber von Hochrisiko-KI	Durchführung einer Grundrechte-Folgenabschätzung vor Einsatz eines Hochrisiko-KI-Systems (Art 27).
Anbieter von GPAI-Modellen	Art 53 regelt Dokumentation, Informationen für nachgelagerte Anbieter, Urheberrechtsstrategie und eine Zusammenfassung der Trainingsinhalte.
Anbieter von GPAI-Modellen mit systemischem Risiko	Art 55 ergänzt die Pflichten nach Art 53 um Modellevaluierungen, Risikobewertung und Risikominderung, Vorfallsmeldungen und Cybersicherheit.
Anbieter von Systemen mit Transparenzpflichten.	Anbieter müssen KI-Systeme für die direkte Interaktion mit Menschen (zB Chatbots) so konzipieren, dass für Betroffene ersichtlich ist, dass sie mit einem KI-System interagieren. Weiters müssen sie KI-generierte Inhalte in maschinenlesbarem Format kennzeichnen. Die Anforderungen an Barrierefreiheit sind einzuhalten (Art 50).
Betreiber von Systemen mit Transparenzpflichten	Betreiber eines Systems zur Emotionserkennung oder biometrischen Kategorisierung müssen dies offenlegen. Deepfakes und Texte von öffentlichem Interesse sind als KI-generiert zu kennzeichnen. Die Anforderungen an Barrierefreiheit sind einzuhalten (Art 50).
Alle Anbieter und Betreiber von KI-Systemen.	Sie fördern KI-Kompetenz nach Art 4. Bei sonstigen Systemen können freiwillige Verhaltenskodizes nach Art 95 hinzukommen.

3.7. Governance, Sanktionen und Haftung

- **EU-Ebene:** Büro für Künstliche Intelligenz (AI Office: KI-Expertise, Überwachung von GPAI-Anbietern, Ausarbeitung und Aktualisierung von Leitlinien) und KI-Gremium (Kooperations- und Koordinationsplattform der Mitgliedstaaten).

- **National:** Marktüberwachungsbehörde zur Ex-post-Kontrolle und Ahndung von Verstößen. In Österreich ist die zuständige Marktüberwachungsbehörde noch zu benennen und ein entsprechendes Umsetzungsgesetz zu erlassen (Stand: Oktober 2026).
- **Sanktionen (Art 99):** insgesamt bis zu 35 Mio. Euro bzw 7 % des weltweiten Jahresumsatzes; bei Verstößen gegen bestimmte Transparenz- und Informationspflichten bis zu 15 Mio. Euro. Es ist auf die Umstände des Einzelfalls Rücksicht zu nehmen (zB Verschuldensgrad und Größe der Einrichtung).
- **Beschwerde (Art 85):** bei der zuständigen Marktüberwachungsbehörde bei behauptetem Verstoß gegen die KI-VO.
- **Haftung:** neue Produkthaftungsrichtlinie (Software als Produkt); die KI-VO wurde in den Anhang der Verbandsklagen-Richtlinie aufgenommen; Datenschutz: Art 82 DSGVO (Schadenersatz); sonstige zivilrechtliche Haftung, zB Schutzgesetze nach § 1311 ABGB.

4. DSGVO und KI-VO: Zusammenspiel

KI-VO und DSGVO **ergänzen einander**, regeln aber unterschiedliche Schutzgüter. In der Praxis fallen viele KI-Anwendungen unter beide Regelwerke gleichzeitig.

	DSGVO	KI-VO
Schutzgegenstand	Personenbezogene Daten und deren Verarbeitung	KI-Systeme nach ihrem Risikopotenzial
Anwendbarkeit	Immer, wenn personenbezogene Daten verarbeitet werden – unabhängig davon, ob KI im Spiel ist (bleibt unberührt)	Bei KI-Systemen – unabhängig davon, ob personenbezogene Daten verarbeitet werden
Zentrale Rolle	Verantwortlicher / Auftragsverarbeiter	Anbieter / Betreiber
Folgenabschätzung	Datenschutz-Folgenabschätzung (Art 35)	Grundrechte-Folgenabschätzung (Art 27), kombinierbar mit der DSFA
Automatisierte Entscheidungen	Art 22: Recht, nicht einer rein automatisierten Entscheidung unterworfen zu sein	Menschliche Aufsicht (Art 14, 26); Recht auf Erläuterung (Art 86)
Datenqualität und Bias	Zweckbindung, Richtigkeit; Art 9 (sensible Daten)	Data Governance (Art 10); ausnahmsweise Verarbeitung sensibler Daten zur Bias-Korrektur (Art 4a KI-VO)

5. Mögliche Anwendungsfelder von KI in der Sozialen Arbeit

Folgende Fallbeispiele stellen mögliche Anwendungsfelder von KI in der Sozialen Arbeit dar. Jedes wirft besondere rechtliche Fragen auf, die in diesem Kapitel praxisnah aufbereitet werden.

Anwendungsfeld	Erklärung	Einstiegsbeispiel
 1. Fallarbeit	Generative KI kann Fachkräfte dabei unterstützen, Informationen zur Lebenssituation zu ordnen und Anamnese, Diagnose sowie Hilfeplanung vorzubereiten. Sie kann außerdem Hinweise auf mögliche Risiken und Gefährdungen liefern.	Eine Sozialarbeiterin lässt Fallnotizen, die personenbezogene Daten beinhalten, strukturieren, um offene Fragen und mögliche Unterstützungsbedarfe für die Hilfeplanung zu sammeln.
 2. Berichtswesen und Administration	Generative KI und mittlerweile zunehmend agentische KI können Dokumentationen auswerten und beim Verfassen oder Überarbeiten von Fallberichten, Besprechungsprotokollen und Förderanträgen helfen. Vorhandene Notizen können dafür geordnet und in verständliche Texte überführt werden.	Eine Fachkraft in der stationären Kinder- und Jugendhilfe lässt Beobachtungsnotizen zu einem Entwurf für den Entwicklungsbericht der halbjährlichen Hilfeplankonferenz zusammenführen.
 3. Contenterstellung	Generative KI unterstützt die Entwicklung pädagogischer Konzepte und die Erstellung von Texten, Bildern und Grafiken. Diese können etwa für Webseiten, soziale Medien, Veranstaltungen oder pädagogische Materialien genutzt werden.	Ein Jugendzentrum entwickelt mit KI einen Flyer für ein Gaming-Event. Die Gestaltung und die Ansprache sollen Jugendliche aller Geschlechter erreichen.
 4. Chatbots im Beratungskontext	Chatbots können Ratsuchenden erste Orientierungen geben und sie zu passenden Angeboten führen, auch außerhalb der Öffnungszeiten. Fachkräfte können sie als Sparringspartner nutzen, um Situationen zu reflektieren und Beratungsgespräche vorzubereiten.	Ein Sozialarbeiter bereitet mit einem KI-Chatbot ein unterstützendes Elterngespräch vor, weil ein Kind wiederholt in schmutziger Kleidung und ohne Jause ins Jugendzentrum kommt.

5.1. Anwendungsfall Fallarbeit

Generative KI kann Fachkräfte dabei unterstützen, Informationen zur Lebenssituation zu ordnen und Anamnese, Diagnose sowie Hilfeplanung vorzubereiten. Sie kann außerdem Hinweise auf mögliche Risiken und Gefährdungen liefern. Dabei ist jedoch zu beachten, dass in diesen Fällen persönliche Informationen in die KI eingegeben werden und die KI einen wesentlichen Beitrag zu Entscheidungen über Diagnose, Risikoeinschätzung und den weiteren Umgang mit betroffenen Klient*innen liefert. Dies kann mit weitreichenden Folgen einhergehen, insbesondere für sog „schutzbedürftige“ oder „vulnerable“ Personen, weshalb sowohl die KI-VO als auch die DSGVO für diesen Fall bestimmte Pflichten vorsehen.

Vulnerabilität bei der Risikoeinschätzung

Vulnerabilität bezeichnet „die Verletzlichkeit oder Verletzbarkeit einer Person, einer sozialen Gruppe, eines Gegenstandes oder eines Systems angesichts bestehender Gefährdungen, Risiken,

Krisen, Stress, Schocks oder bereits eingetretener belastender Ereignisse“.[18] Vulnerable Zielgruppen sind in der Sozialen Arbeit demnach Personen oder Gruppen, die als in besonderem Maß verletzbar, gefährdet oder schutzbedürftig gelten. Vulnerabilität ist in der Fallarbeit mitzudenken und findet auch im Recht ihren Niederschlag.

- Doch weder das Unionsrecht noch das österreichische Recht enthalten eine **allgemeine Legaldefinition** der Vulnerabilität. Der Begriff ist über mehrere Rechtsakte verstreut und muss kontextabhängig rekonstruiert werden.
- Die KI-VO verweist immer wieder auf die Schutzbedürftigkeit von Personen aufgrund von Status, Autorität, Wissen, wirtschaftlichen oder sozialen Umständen (zB Armut, ethnische und religiöse Minderheiten), Alter sowie Behinderung.
- Indikatoren für Vulnerabilität sind meist ein **Machtungleichgewicht**, mangelnde Einsichtsfähigkeit in oder **mangelndes Wissen** um einen Prozess und **Ungleichbehandlungen** aufgrund von Herkunft, Geschlecht oder sozialer Klasse. Das bedeutet, dass sich in der Praxis besondere Risiken ergeben, wenn schutzbedürftige Personen (zB aufgrund ihrer Herkunft, einer Behinderung oder ihres Alters) einem KI-Einsatz unterliegen, durch den sie diskriminiert werden könnten. Problematisch ist außerdem, wenn Personen einem KI-Einsatz ausgeliefert sind, ohne überhaupt davon zu wissen.
- Vulnerabilität ist insbesondere bei **Folgenabschätzungen** mitzudenken (Art 35 DSGVO bzw Art 27 KI-VO), in denen die Folgen einer KI-Anwendung aus unterschiedlichen Perspektiven beleuchtet und Risikominderungsmaßnahmen erarbeitet werden (siehe sogleich).

Datenschutz-Folgenabschätzung (DSFA)

Birgt eine Datenverarbeitung – insbesondere bei Verwendung **neuer Technologien** – voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, führt der Verantwortliche **vorab** eine Abschätzung der Folgen durch.[19] Erforderlich ist sie insbesondere bei:

- systematischer und umfassender Bewertung persönlicher Aspekte auf Basis automatisierter Verarbeitung einschließlich **Profiling**,
- umfangreicher Verarbeitung **besonderer Kategorien** personenbezogener Daten oder strafrechtsbezogener Daten,
- systematischer **umfangreicher Überwachung** öffentlich zugänglicher Bereiche.

Nach der österreichischen DSFA-Verordnung (§ 2 Abs 2 Z 4) gehören dazu auch Verarbeitungen unter Nutzung oder Anwendung neuer bzw neuartiger Technologien, insbesondere durch den **Einsatz von künstlicher Intelligenz**. Die DSGVO hebt außerdem die Schutzbedürftigkeit von Kindern als Faktor bei der Risikobewertung hervor (Erwägungsgrund 75).

[18] Juliane Noack-Napoles: Vulnerabilität als Deutungshorizont sozialer Probleme am Beispiel von Einsamkeit. Näheres zum Begriff der „Vulnerabilität“ kann im eigenen Projekt-Glossar nachgelesen werden, abrufbar unter: https://digitalesozialearbeit.github.io/socialai-knowledge-hub/#/glossar/.

[19] Vgl dazu Art 35 DSGVO.

Fazit für die Praxis

Wer KI-Tools zur Verarbeitung von Klient*innendaten (bspw über Gesundheit oder Straftaten) in der Fallarbeit (zB zur Diagnoseunterstützung oder Gefährdungseinschätzung) einsetzen will, sollte grundsätzlich davon ausgehen, dass eine DSFA erforderlich ist, und diese **vor** dem Einsatz durchführen.

Grundrechte-Folgenabschätzung (GRFA)

Betreiber müssen bei der ersten Verwendung eines **„eigenständigen" Hochrisiko-KI-Systems** nach Anhang III KI-VO (außer kritische Infrastruktur) abschätzen, welche Auswirkungen der KI-Einsatz auf die Grundrechte haben kann.[20] Die Pflicht gilt nur für bestimmte Betreiber:

- Einrichtungen des öffentlichen Rechts,
- private Einrichtungen, die **öffentliche Dienste** erbringen,
- Betreiber von Hochrisiko-KI-Systemen nach Anhang III Nr 5 lit b und c (Kreditwürdigkeitsprüfung, Preisbildung bei Lebens- und Krankenversicherung).

Welche Hochrisiko-Systeme kommen im Sozialbereich infrage? KI-Systeme zur Beurteilung des Anspruchs auf grundlegende öffentliche Unterstützungsleistungen und -dienste (Anhang III Nr 5a). Die Entwurfsleitlinien der Europäischen Kommission zur Einstufung von Hochrisiko-KI[21] nennen „Social Services" (mit Bezug zu Kinderbetreuung) und als Beispiele die Priorisierung bei der Zuteilung von Hauspflege-Leistungen oder Chatbots, mit denen Sachbearbeiter*innen Anträge auf wesentliche Pflegeleistungen bewerten. Die Leitlinien befinden sich noch im Entwurfsstadium und sind weiters nicht rechtsverbindlich, bieten allerdings wertvolle Orientierung zur Einstufung von Hochrisiko-KI. Unter Umständen ist auch an Emotionserkennung im Sinne von Anhang III Nr 1c zu denken. Sofern öffentliche Einrichtungen KI in Bewerbungsverfahren oder zur Leistungsbeurteilung einsetzen, kommt auch der Hochrisiko-KI-Einsatz nach Anhang III Nr 4 in Betracht.

Inhalt der Abschätzung:

- Beschreibung der Verfahren, in denen das System bestimmungsgemäß verwendet wird, sowie von Zeitraum und Häufigkeit des Einsatzes
- Kategorien betroffener Personen und spezifische Schadensrisiken für diese Gruppen
- Umsetzung der Maßnahmen zur menschlichen Aufsicht laut Betriebsanleitung
- Maßnahmen bei Eintritt der Risiken (zB interne Unternehmensführung, Beschwerdemechanismen)

Eine Kombination mit anderen Folgenabschätzungen (zB als Ergänzung zur DSFA) ist möglich und es besteht eine laufende Aktualisierungspflicht. Das AI Office arbeitet an einem Musterfragebogen. Bis dahin bieten der ELI-Report[22] und das kanadische „Algorithmic Impact Assessment"[23] Orientierung.

[20] Vgl Näheres in Art 27 KI-VO.
[21] https://digital-strategy.ec.europa.eu/de/library/draft-commission-guidelines-classification-high-risk-ai-systems.
[22] https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Impact_Assessment_of_ADMSs_Used_by_Public_Administration.pdf.
[23] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.

Anwendungsfall Fallarbeit

Beim Anwendungsfall der Fallarbeit würde höchstwahrscheinlich kein Hochrisiko-KI-System vorliegen, wenn das System lediglich zur Strukturierung von Informationen oder zur vorbereitenden Hilfeplanung eingesetzt wird. Ist das System für den Zweck der Anamnese- oder Diagnoseerstellung gedacht, könnte ein Medizinprodukt nach Art 6 Abs 1 KI-VO vorliegen, das ein Hochrisiko-KI-System darstellt (siehe dazu noch näher Abschnitt 5.4. zur Grenzfrage, ob Chatbots, die Gesundheitsfragen beantworten, Medizinprodukte sind).

Da es sich bei Medizinprodukten allerdings nicht um Anhang-III-Systeme handelt, unterliegen ihre Betreiber nicht der Pflicht zur Durchführung einer GRFA.

Automatisierte Einzelentscheidungen (Art 22 DSGVO)

Art 22 DSGVO enthält ein Verbot, Personen **einer rein automatisierten Entscheidungsfindung zu unterwerfen**, wenn diese rechtliche Folgen hat oder die Person erheblich beeinträchtigt (zB Ablehnung eines Antrags, einer Bewerbung oder des Zugangs zu Leistungen). Dabei handelt es sich um Entscheidungen, die ohne wesentliches menschliches Zutun getroffen werden. **Das Verbot gilt nicht, wenn**

- die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist,
- aufgrund von Rechtsvorschriften der EU oder eines Mitgliedstaats zulässig ist oder
- auf ausdrücklicher Einwilligung der Betroffenen beruht (die echte Willensbildungsfreiheit voraussetzt).

Umstritten ist, wann tatsächlich eine *ausschließlich automatisierte* Entscheidung vorliegt: Werden algorithmische Empfehlungen blind befolgt, oder werden sie kritisch hinterfragt und prüft die Fachkraft eigenständig? Der **Europäische Gerichtshof (EuGH)** hat klargestellt, dass eine Einrichtung Art 22 auch dann unterliegt, wenn automatisiert berechnete Punktewerte („Score-Werte“ oder „Scoring“) maßgeblich eine nachgelagerte menschliche Entscheidung determinieren.[24] Beispiele für solche Praktiken wären Entscheidungen über die Vergabe von Leistungen oder Bewerbungsselektionen, die wesentlich auf zuvor errechneten Eignungswerten beruhen. Ein Entscheidungsprozess unterliegt somit dann dem Anwendungsbereich von Art 22, wenn er *maßgeblich* auf einer automatisierten Verarbeitung beruht und kein wesentliches menschliches Eingreifen mehr vorgesehen ist. **In diesem Fall ist eine derartige Datenverarbeitung verboten, außer es liegt eine der drei oben genannten Ausnahmen von dem Verbot vor.**

[24] Vgl die Entscheidung: EuGH, 07. Dezember 2023, *SCHUFA*, C-634/21.

Praxis-Tipp

Eine „Pro-forma"-Prüfung durch eine Fachkraft genügt nicht, um den Anwendungsbereich von Art 22 auszuhebeln. Dazu muss die Fachkraft die Entscheidung eigenständig prüfen, davon abweichen können und über die dafür erforderliche Kompetenz und Zeit verfügen. Ein Beispiel für einen derartigen Entscheidungsprozess, bei dem der Anwendungsbereich des Art 22 nicht eröffnet war, stellt der Fall des Arbeitsmarktchancen-Assistenzsystems „AMAS" des österreichischen Arbeitsmarktservice dar. Dieses bewertete die Arbeitsmarktchancen Arbeitssuchender mit einem Punktewert als Grundlage für die Ressourcenzuweisung. Laut dem Bundesverwaltungsgericht (BVwG) handelte es sich um keinen Anwendungsfall der ausschließlich automatisierten Entscheidungsfindung, da die AMS-Berater*innen vom algorithmisch berechneten „AMAS-Wert" abweichen konnten und weitere Faktoren bei der Entscheidung über die Ressourcenzuweisung berücksichtigten, insbesondere persönliche Gespräche mit den betroffenen Arbeitssuchenden. Ihre Beteiligung war somit nicht bloß formal, sondern die Letztentscheidung verblieb bei den Berater*innen, weshalb es sich um keine „ausschließlich automatisierte Entscheidung" handelte.[25]

Im Falle einer zulässigen automatisierten Entscheidungsfindung haben Betroffene bestimmte Rechte[26]:

- Das Recht auf Eingreifen einer Person
- Das Recht auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung
- Ein Auskunftsrecht über die involvierte Logik, Tragweite und Auswirkungen der Entscheidung
- Zusätzlich muss der Verantwortliche die Betroffenen vorab über die Entscheidungsfindung bzw Datenverarbeitung in Kenntnis setzen

Bedeutung für den Anwendungsfall:

Bei Risiko-Scoring-Systemen zur Gefährdungseinschätzung könnte es sich um automatisierte Einzelentscheidungen handeln, wenn diese negative Konsequenzen für Betroffene haben und kein menschliches Eingreifen erfolgt. Dann wäre der Anwendungsbereich von Art 22 DSGVO eröffnet und es müsste eine entsprechende Rechtsgrundlage für den Einsatz des Systems vorliegen. Einrichtungen haben Betroffene dann vorab über die Datenverarbeitung zu informieren.

Werden solche Entscheidungen von oder unter Mithilfe von **Hochrisiko-KI-Systemen nach Anhang III KI-VO** getroffen und haben ähnliche Auswirkungen auf Betroffene, kommt diesen ein **Recht auf Erklärung**[27] gegen den Betreiber zu. Dieser hat ihnen sodann klare und aussagekräftige Informationen über die wesentlichen Entscheidungselemente und die Rolle des KI-Systems im Entscheidungsprozess zu übermitteln. Vorab sind Betroffene außerdem über den KI-Einsatz zu informieren und – sofern es sich um einen Hochrisiko-KI-Einsatz am Arbeitsplatz handelt – die betroffenen Beschäftigten und ihre Vertretung darüber in Kenntnis zu setzen (**Vorab-Informationspflichten** nach den Art 26 Abs 7 und 11 KI-VO).

25 Vgl BVwG 1. 9. 2025, W256 2235360-1/36E.
26 Vgl Art 13-15 sowie Art 22 Abs 3 DSGVO.
27 Siehe Artikel 86 KI-VO. Hier ist von einem „Recht auf Erläuterung der Entscheidungsfindung im Einzelfall" die Rede, das jedoch immer wieder als „Recht auf Erklärung" bezeichnet wird.

5.2. Anwendungsfall Berichtswesen und Administration

Generative KI und mittlerweile zunehmend agentische KI können Dokumentationen auswerten und beim Verfassen oder Überarbeiten von Fallberichten, Besprechungsprotokollen oder Förderanträgen helfen. Ein Beispiel wäre eine Fachkraft der stationären Kinder- und Jugendhilfe, die sich Beobachtungsnotizen für einen Entwicklungsbericht oder für einen Antrag auf Förderung zusammenführen lässt.

Agentische KI

Ein **KI-Agent** ist ein autonomes Softwaresystem, das eigenständig Ziele verfolgt, indem es seine Umgebung wahrnimmt, Handlungen plant und ausführt, sodass diese die Umgebung tatsächlich beeinflussen – in einer fortlaufenden Schleife, bis das Ziel erreicht ist. Sein „Motor" ist meist ein Large Language Model (LLM). Kernmerkmale sind Wahrnehmung, Planung und Gedächtnis, Werkzeugnutzung (zB Websuche, Code-Ausführung, Dateizugriff), tatsächliche Umgebungsbeeinflussung sowie Handlung und Iteration. Beispiel: „Recherchiere die drei günstigsten Flüge und erstelle eine Übersichtstabelle." – der Agent ruft eine Flugsuch-API auf, filtert, sortiert und liefert eine Tabelle.

Für das Berichtswesen ist das relevant, weil KI-Agenten Dokumente lesen, Daten zusammenführen und Berichte erstellen oder versenden können. Rechtlich gilt:

- Die **Einordnung nach der KI-VO hängt von KI-Kategorie und Verwendungszweck ab** und davon, auf welcher Technologie der Agent basiert.
- In der Regel dient ein LLM als „Motor" bzw „Gehirn", welches als KI-Modell mit allgemeinem Verwendungszweck (**GPAI-Modell**) nach der KI-VO einzustufen ist. Ist es in ein KI-System integriert, das eine Vielzahl von Zwecken erfüllen kann, liegt ein **GPAI-System** vor.
- Die weitere Einstufung anhand der **Risikoklassen** der KI-VO hängt vom Verwendungszweck ab.[28]
- **Aktuelles Problem „behavioural drift":** Anpassung während des Lebenszyklus und autonome Erschließung neuer Aufgabenbereiche und Einsatzzwecke stellen die rechtliche Beurteilung vor neue Herausforderungen.[29]

Rollenabgrenzung und Drittlandthematik

Wer ist was?	Konsequenz
Verantwortlicher *(Art 4 Z 7 DSGVO)*	Die Einrichtung (der Träger) bestimmt Zweck und Mittel der Datenverarbeitung, also beispielsweise den Zweck der Zusammenführung von Dokumenten und Daten durch das Mittel des agentischen KI-Systems.

[28] Nähere Informationen unter: *Fleischmann*, KI-Agenten-Systeme: Einordnung in die KI-Verordnung, RDi 2025, 193.
[29] Vgl dazu insbesondere die Auseinandersetzung in: *Nannini et al,* AI Agents under EU Law, arXiv 2026, 1.

Wer ist was?	Konsequenz
Mitarbeiter*in	Wird die Person im Rahmen ihrer beruflichen Aufgaben tätig, hat sie keine eigenständige datenschutzrechtliche Rolle und ihr Verhalten ist der Einrichtung zuzurechnen.
Auftragsverarbeiter *(Art 4 Z 8, Art 28 DSGVO)*	Ein KI-Anbieter kann Auftragsverarbeiter sein, wenn personenbezogene Daten (zB von Klient*innen) verarbeitet werden, auch wenn die Verarbeitung nur zur Textgenerierung erfolgt. Verarbeitet der KI-Anbieter die Daten nur auf Weisung der verantwortlichen Einrichtung und entscheidet selbst nicht über das „Wie“ und „Wozu“, ist er Auftragsverarbeiter. Erforderlich: Auftragsverarbeitervereinbarung zwischen Verantwortlichem und KI-Anbieter.
Drittlandanbieter	Es ist zu prüfen, ob eine Drittlandübermittlung (Länder außerhalb der EU) vorliegt und ob sie gerechtfertigt ist. Die DSGVO sieht dazu bestimmte zusätzliche Anforderungen vor (Art 44 ff) und lässt einen Datentransfer nur unter bestimmten Voraussetzungen zu (zB in die USA, sofern ein Unternehmen unter dem Data Privacy Framework zertifiziert ist).

5.3. Anwendungsfall Contenterstellung

Generative KI kann zur Entwicklung pädagogischer Konzepte und zur Erstellung von Texten, Grafiken und Bildern eingesetzt werden, die für Webseiten, soziale Medien, Veranstaltungen oder pädagogische Materialien genutzt werden können. Sobald KI-generierte Inhalte veröffentlicht werden, entstehen Transparenzrisiken (zB weil die Inhalte für echt gehalten werden könnten), welche die KI-VO durch bestimmte Transparenzpflichten adressiert.

Transparenz- und Kennzeichnungspflichten (Art 50 KI-VO)

Was?	Wer?	Beispiel
Information, dass man mit einem KI-System direkt interagiert	Anbieter	Chatbots, die als erste Anlaufstelle einer Einrichtung mit Klient*innen interagieren.
Information über Emotionserkennungs- bzw biometrische Kategorisierungssysteme	Betreiber	Systeme zur Ableitung und Erkennung von Emotionen wie Wut, Trauer, Scham
Information über Deepfakes (künstlich erzeugte oder manipulierte Inhalte)	Betreiber	KI-Bilder realer Personen oder KI-generierte Personen, die echten Menschen ähnlich erscheinen. Selbiges gilt für Orte, Einrichtungen und Ereignisse. Dies ist für die Soziale Arbeit von Bedeutung, wenn echt wirkende KI-generierte Personen oder Ereignisse für Kampagnen oder Informationsmaterial verwendet werden.

Was?	Wer?	Beispiel
Maschinenlesbare Kennzeichnung für den Output generativer Systeme	Anbieter	Hinterlegung von Metadatenidentifizierungen oder Wasserzeichen.[30]
Information über künstlich generierte oder manipulierte Texte, die veröffentlicht werden, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, sofern keine redaktionelle Kontrolle erfolgt.	Betreiber	Veröffentlichte Berichte, Presseaussendungen, Informationen auf offiziellen Social-Media-Kanälen. Dies ist für die Soziale Arbeit besonders relevant.

Das AI Office hat einen **Verhaltenskodex zur Transparenz KI-generierter Inhalte** vorgestellt.[31] Als technische Lösungen genannt werden Wasserzeichen, Metadatenidentifizierungen (zB digitale Signatur), kryptografische Methoden, Protokollierung, Fingerabdrücke und erkennbare Kennzeichnungen „by default" gegen Deepfakes.

Urheberrecht im KI-Zeitalter

Bei KI-generierten Bildern, Texten oder Audioinhalten stellen sich urheberrechtliche Fragen: Wer ist geschützt? Was ist geschützt? Wovor? Wie lange? Die Grundlagen:

- **§ 1 Abs 1 UrhG:** Werke sind eigentümliche geistige Schöpfungen auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste und der Filmkunst. Erforderlich ist ein Mindestmaß an Individualität und Originalität. **Urheber können nur natürliche Personen sein**.
- **Nicht geschützt:** Tatsachen, abstrakte Ideen und künstlerischer Stil (beachte jedoch Muster- und Markenschutz).
- Schutzdauer grundsätzlich bis zu **70 Jahre nach dem Tod** des Urhebers. Der Schutz beginnt automatisch mit der Entstehung des Werks.

Die zwei urheberrechtlichen Hauptfragen im Zusammenhang mit KI betreffen sowohl

1) **Anbieter** in Bezug auf die Verwendung urheberrechtlich geschützten Materials zum KI-Training als auch
2) **Betreiber** im Hinblick auf den rechtlichen Status von Eingaben und KI-generierten Ausgaben.

1) Anbieter und KI-Training: Training mit urheberrechtlich geschütztem Material in großem Ausmaß ist nach überwiegender Ansicht eine Vervielfältigung nach § 15 UrhG und grundsätzlich **erlaubnispflichtig**. Davon besteht eine Ausnahme für das Text- und Data-Mining (§ 42h UrhG): KI-Training mit urheberrechtlich geschützten Inhalten ist demnach ohne gesonderte Erlaubnis zulässig, wenn es

(a) zu Zwecken der wissenschaftlichen Forschung geschieht oder

(b) für den eigenen Gebrauch, sofern der Rechteinhaber die Nutzung nicht ausdrücklich untersagt hat (zB maschinenlesbarer Nutzungsvorbehalt)

[30] Siehe hierzu beispielsweise die Kennzeichnung von KI-generierten Inhalten durch den KI-Anbieter Anthropic: https://support.claude.com/de/articles/16266773-wie-claude-ki-generierte-inhalte-kennzeichnet.
[31] https://digital-strategy.ec.europa.eu/de/policies/code-practice-ai-generated-content.

und der Zugang zu den Inhalten rechtmäßig ist.

2) Betreiber und der Status von Ein- und Ausgaben:

Inputs: Was gebe ich in die KI ein?	Outputs: Was mache ich mit dem Ergebnis?
• Prompts sind die Schnittstelle zwischen menschlicher Kreativität und maschineller Generierung. • Urheberrechtlich geschützt sind sie nur, wenn sie eine individuelle, originelle geistige Schöpfung sind – es kommt auf den Einzelfall an. • Funktionale Prompts („Schreibe eine Liste mit fünf Vorteilen von Recycling"): in der Regel nein. • Kreative Prompts: ja, wenn individueller Stil, sprachliche Gestaltung oder eine originelle Idee sichtbar wird.	• Urheber kann nur ein Mensch sein (§ 10 Abs 1 UrhG: „Schöpfung des menschlichen Geistes"). • Reine „Maschinenschöpfungen" können daher nicht urheberrechtlich geschützt sein. • Schwierige Abgrenzung, wenn KI als Werkzeug für menschliche Schöpfung genutzt wird. • Folge für die Praxis: Ergebnisse sind evtl nicht urheberrechtlich geschützt; offen ist zB, was gilt, wenn verschiedene Nutzer*innen ähnliche Ergebnisse erzeugen.

Beispiel: Werbebild „im Stil von Banksy"

Eine Agentur lässt ein KI-Tool ein Werbebild im Stil von Banksy erstellen. Reproduziert der Output Bildelemente des Originals, kann die Agentur Urheberrechte verletzen und dafür haften. Der bloße Stil ist zwar nicht geschützt – konkrete Werkelemente sind es aber sehr wohl. Auch beim „Pastiche"-Fall (Sampling; EuGH 14.04.2026, C-590/23) im Zusammenhang mit Musikwerken zeigt sich: Schon kurze übernommene Tonsequenzen können eine Urheberrechtsverletzung sein, außer sie werden in geänderter und nicht wiedererkennbarer Form eingefügt.

5.4. Anwendungsfall Chatbots im Beratungskontext

Chatbots können Ratsuchenden erste Orientierungen geben und sie zu passenden Angeboten führen, auch außerhalb der Öffnungszeiten. Fachkräfte können sie als Sparringpartner nutzen, um Situationen zu reflektieren und Beratungsgespräche vorzubereiten. Eine Fachkraft könnte beispielsweise mit einem Chatbot ein Eltern-Kind-Gespräch vorbereiten, weil das Kind wiederholt in schmutziger Kleidung und ohne Jause ins Zentrum kommt oder weil ein Kind traurig und antriebslos wirkt.

Kennzeichnung der Chatbot-Interaktion (Art 50 Abs 1 KI-VO)

Anbieter müssen sicherstellen, dass KI-Systeme, die für die **direkte Interaktion mit natürlichen Personen** bestimmt sind, so konzipiert werden, dass die Betroffenen **informiert werden, dass sie mit einem KI-System interagieren** – es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich.

KI-Haftung

Wer übernimmt die Haftung, wenn ein Chatbot falsche Ausgaben liefert oder in der persönlichen Interaktion Probleme verstärkt?

Anbieterseite	Betreiberseite (Träger)
Wer ist Anbieter? Das Unternehmen, das den KI-Chatbot entwickelt und auf den Markt bringt (zB OpenAI, Google oder spezialisierte Anbieter sozialer Fachlösungen). Produkthaftung: Nach der neuen EU-Produkthaftungsrichtlinie fällt KI als Software eindeutig unter die Produkthaftung – auch als Software-as-a-Service. • Chatbot mit mangelhaften Sicherheitsmechanismen = fehlerhaftes Produkt • Haftung tritt auch dann ein, wenn Produktfehler durch fehlende Updates entstehen – Anbieter müssen ihre Systeme aktiv sicher halten • Pauschaler Haftungsausschluss durch Hinweise wie „KI-generiert" ist rechtlich wirkungslos	• Vertragliche Haftung (§§ 1295, 1313a ABGB): Der Träger haftet für KI-bedingte Schäden im Rahmen des Betreuungs- oder Beratungsverhältnisses. Der Chatbot könnte als Erfüllungsgehilfe des Trägers nach § 1313a ABGB eingestuft werden oder dieser muss ihn sich als Tool zurechnen lassen. • Deliktische Haftung (§ 1295 ABGB): kann greifen, wenn fehlerhafte KI-Ausgaben in absolut geschützte Rechtsgüter eingreifen (insbesondere Leib und Leben). • Sachverständigenmaßstab (§ 1299 ABGB): Fachkräfte, die einen KI-Chatbot im Beratungskontext einsetzen, könnten an diesem erhöhten Berufsstandard gemessen werden.

Halluzinationen und Automation Bias

Große Sprachmodelle generieren Text auf Basis statistischer Wahrscheinlichkeiten – nicht auf Basis von Faktenprüfung. **Halluzinationen bzw Konfabulationen** entstehen, wenn das Modell plausibel klingende, aber faktisch falsche oder erfundene Inhalte ausgibt (nicht existente Urteile, fiktive Quellen, falsche Norminhalte).

Fallbeispiel: KI-Halluzinationen vor Gericht (OGH 7.10.2025, 14 Os 95/25i)

Nach einer Verurteilung seines Mandanten wegen Suchtgifthandels erhob ein Anwalt Nichtigkeitsbeschwerde – offenbar unter Einsatz von KI. Die KI erfand nicht existente OGH-Entscheidungen als Quellen und stellte falsche Verfahrensergebnisse als Sachverhalt dar. Der OGH hielt fest, dass offenbar ohne fachliche Kontrolle durch „künstliche Intelligenz" erstellte Vorbringen den rechtlichen Erfordernissen nicht ansatzweise genügen. Folge: Zurückweisung wegen formeller Mängel ohne inhaltliche Befassung und der Angeklagte musste die Verfahrenskosten tragen.

Automation Bias bezeichnet die Tendenz, sich in bestimmten Situationen übermäßig auf automationsunterstützte Entscheidungssysteme zu verlassen, ohne deren Output kritisch zu prüfen. Empfehlungen werden dann eher für gültig gehalten, auch wenn sie falsche oder unvollständige Informationen liefern. Kritisches Denken wird durch das Vertrauen in „maschinelle Autorität" ersetzt. Die KI-VO nimmt darauf mehrfach Bezug:

Art 4	KI-Kompetenzpflicht für Belegschaft, die mit KI arbeitet
Art 14	Menschliche Aufsicht: Gewährleistung, sich einer möglichen Neigung zu automatischem oder übermäßigem Vertrauen in eine KI-Ausgabe bewusst zu bleiben
Art 15	Genauigkeit: Risiko für verzerrte Ausgaben soll beseitigt bzw so gering wie möglich gehalten werden
Art 50	Kennzeichnungspflicht für KI-generierte Texte und Inhalte in bestimmten Kontexten

Fallbeispiel: Kinderbetreuungsgeld-Skandal („Toeslagenaffaire" in den Niederlanden)

Das niederländische Finanzamt hatte digitale Modelle (Regressionsanalyse) zur Effizienzsteigerung bei der Erkennung von Sozialbetrug entwickelt. Unzählige Eltern wurden zu Unrecht unter Generalverdacht gestellt, betrügerische Leistungsanträge gestellt zu haben. Mehrere zehntausend Euro mussten jeweils zurückgezahlt werden. Folgen waren Privatkonkurse, der Entzug von Sorgerechten und mehrere Suizide. Der Skandal führte 2021 zum Rücktritt der Regierung.[32]

Auf das Fallbeispiel von Chatbots im Beratungskontext der Sozialen Arbeit bezogen könnte ein Automation Bias vorliegen, wenn die Fachkraft, die ein Eltern-Kind-Gespräch aufgrund der traurigen Stimmung eines Jugendlichen oder der schmutzigen Kleidung eines Kindes sucht, sofort Alkoholismus, psychische Erkrankung oder sexuellen Missbrauch in der Familie vermutet, weil der Chatbot zu diesem Schluss gelangt ist.

Offene Rechtsfrage: Sind Chatbots, die medizinische oder therapeutische Fragen beantworten, Medizinprodukte?

Wenn ein KI-Chatbot wie ChatGPT auf Gesundheitsfragen konkrete diagnostische oder therapeutische Hinweise gibt: Ist er ein Medizinprodukt nach der Medizinprodukte-Verordnung (MPVO) und damit ein Hochrisiko-KI-System nach Art 6 Abs 1 lit a KI-VO?

Pro Einstufung als Medizinprodukt	Kontra Einstufung
• Die Zweckbestimmung folgt dem tatsächlichen Verhalten, nicht dem Marketing; ein Disclaimer „Dies ist kein Medizinprodukt" schützt nicht. • Die Gesamtschau der Kommunikationsverläufe entscheidet • Der Chatbot erfüllt „Anhaltsbegriffe" (diagnostizieren, interpretieren) und „Anhaltsfunktionen" (Entscheidungsunterstützung).	• Maßgeblich ist die subjektive Zweckbestimmung des Herstellers (zB in Gebrauchsinformationen) → „Definitionsmacht" des Herstellers • EuGH-Urteil: Software für allgemeine Zwecke ist kein Medizinprodukt. • Erwägungsgrund 19 MPVO (keine Software für allgemeine Zwecke oder für Lifestyle und Wohlbefinden).

[32] Quellen: *BMKÖS,* Leitfaden Digitale Verwaltung, Ethik und Recht, 32; https://www.derstandard.de/story/3000000272188/steuert-ki-die-verwaltung-kann-das-mitunter-gefaehrlich-werden.

Fazit für die Soziale Arbeit: Die Einordnung ist derzeit ungeklärt und gegebenenfalls gerichtlich zu klären. Anbieter, Betreiber und Nutzer*innen von Chatbots müssen sich der Risiken einer Einstufung als Medizinprodukt und Hochrisiko-KI-System bewusst sein.

5.5. Exkurs: Blackbox, Bias und Diskriminierung

KI-Systeme agieren autonom, operieren allerdings häufig in undurchsichtiger Weise, dh viele ihrer „Denkprozesse" sind für Menschen nicht nachvollziehbar („Black-Box-Problem"). Ihnen werden oft besondere logische Fähigkeiten zugeschrieben, obwohl sie nur auf Grundlage statistischer Wahrscheinlichkeiten arbeiten (ironische Bezeichnung: „stochastischer Papagei"). Folgen können fehlerhafte Entscheidungen und Diskriminierung sein.

Mögliche Fehlerquellen: (1) die Datengrundlage („Garbage in – Garbage out"; die KI sucht Muster in vorhandenen Daten und leitet daraus Entscheidungen ab) und (2) Fehler in der KI selbst bei der Datenverarbeitung, ohne dass diese für Nutzer*innen nachvollziehbar sind.

Beispiel: Ein Bewerbungs-Tool, das auf eine Mitarbeiterhistorie zurückgreift, in der bisher nur Männer eingestellt wurden, benachteiligt Frauen. Ein weiteres Beispiel ist die US-Software „COMPAS" zur Rückfallprognose von strafrechtlich verurteilen Personen, deren Bewertungen als verzerrt kritisiert wurden, da das System Menschen einer bestimmten Ethnie stärker benachteiligte. Derartige Verzerrungen bezeichnet man auch als „Bias". Zwar beruhen diese oftmals auf bereits in der Gesellschaft vorherrschenden Vorurteilen, die durch die KI lediglich repliziert werden. Beim wiederholten Training von KI mit diesen Daten können sich bestehende Verzerrungen jedoch verstärken und die Vielfalt abgebildeter Lebensrealitäten verringern, wodurch diskriminierende Ergebnisse wahrscheinlicher werden.

Bias kann sich auf vielerlei Weise manifestieren:

Phase des KI-Lebenszyklus	Bias-Typ	Erklärung und Beispiel
Datenerhebung	Historical Bias	Vergangene Diskriminierung wird als Normalzustand kodiert (zB weniger Frauen in Führungspositionen, daher bevorzugt ein Bewerbungstool eher Männer).
Feature-Auswahl	Representation Bias	Unterrepräsentierte Gruppen fehlen oder sind verzerrt abgebildet (zB oft nur „westliche" Datensets).
Modelltraining	Measurement Bias	Entsteht durch die Art, wie Variablen gemessen werden (zB COMPAS: „Kriminalität von Familienmitgliedern" als Messgröße).
Deployment	Aggregation Bias	Ein Modell für alle ignoriert relevante Gruppenunterschiede (zB variieren bestimmte gesundheitliche Werte je nach Ethnie und Geschlecht).

Merke: Bias entsteht nicht zufällig, sondern systematisch an bestimmten Stellen im KI-Lebenszyklus und verstärkt sich durch Feedback-Loops. Praktisch ist es kaum möglich, alle Bias-Quellen zu korrigieren. Ein effektives „De-Biasing" zielt auf bestmögliche Bias-Minderung.

Rechtliche Vorschriften, um dem entgegenzutreten:

- **De-Biasing mit sensiblen Daten (Art 4a KI-VO):** Ausnahmsweise dürfen sensible Daten (Art 9 DSGVO) zur Erkennung und Korrektur von Verzerrungen verarbeitet werden. Dies allerdings nur, wenn die Verarbeitung „unbedingt erforderlich" ist und zB nicht mit synthetischen oder anonymisierten Daten erfolgen kann. Sensible Daten sind nach Zweckerreichung zu löschen und es besteht keine Rechtsgrundlage für KI-Training oder Performance-Verbesserung. Diese Vorschrift gilt für Anbieter und Betreiber aller KI-Systeme und -Modelle.
- **Antidiskriminierungsrecht:** Das Gleichbehandlungsgesetz (GlBG) gilt im Beschäftigtenkontext und schützt unter anderem vor Diskriminierungen nach Geschlecht, ethnischer Zugehörigkeit, Religion/Weltanschauung, Alter und sexueller Orientierung. Demnach sind sowohl die unmittelbare als auch mittelbare Diskriminierung aufgrund dieser Merkmale verboten. Bei Verletzung besteht ein Schadenersatzanspruch. Beispiel: Der Einsatz von KI im Bewerbungsprozess und die Miteinbeziehung von sogenannten „Proxy-Merkmalen" (zB Postleitzahl als Hinweis auf ethnische Zugehörigkeit) können mittelbare Diskriminierung begründen.

6. Checkliste: Vor dem Einsatz von KI-Tools

Die folgenden Leitfragen eignen sich als Grundlage für Teamgespräche, interne KI-Richtlinien und die Vorbereitung eines konkreten KI-Einsatzes.

Zweck und Nutzen

	Frage	Rechtsbezug
☐	Welche konkrete Tätigkeit oder welcher Arbeitsschritt soll durch KI unterstützt werden, und welches Ergebnis wird erwartet?	Zweckbindung DSGVO, zweckgemäßer Einsatz (Art 26 KI-VO)
☐	Wer nutzt das KI-Tool, und wer entscheidet über die Nutzung?	Verantwortlichkeit, Rollenverteilung, KI-Kompetenz (Art 4)

Dateninput und Datenweg

	Frage	Rechtsbezug
☐	Werden personenbezogene, sensible oder besonders schutzwürdige Informationen eingegeben (Gesundheit, Behinderung, Herkunft, Geschlecht, Alter, Familie, Straftaten)?	Art 4 Z 1, 9, 10 DSGVO
☐	Sind Klient*innen direkt oder indirekt identifizierbar?	Art 4 Z 1 DSGVO
☐	Wissen Klient*innen, wo die Daten landen (Organisation, Anbieter, Ausland)?	Art 44 ff DSGVO, Art 13, 14 DSGVO
☐	Wird ein privates oder ein organisationsseitig freigegebenes Tool genutzt?	Rollen, Verantwortlicher
☐	Liegt ein Erlaubnistatbestand vor? Besteht eine Auftragsverarbeitervereinbarung, und ist KI-Training mit Klient*innendaten ausgeschlossen?	Art 6, Art 9, Art 10, Art 28 DSGVO Zweckbindung
☐	Wurde geprüft, ob eine Datenschutz-Folgenabschätzung (und ggf Grundrechte-Folgenabschätzung) erforderlich ist?	Art 35 DSGVO, Art 27 KI-VO

Einfluss auf Einschätzungen und Entscheidungen

	Frage	Rechtsbezug
☐	Wird KI nur als Entwurfs-, Strukturierungs- oder Formulierungshilfe genutzt, oder beeinflusst sie Bewertungen, Risikoeinschätzungen, Hilfeplanung, Entscheidungen oder Beratung?	Art 22 DSGVO, Art 6 Abs 3 KI-VO
☐	Wer prüft den Output, bevor er verwendet, weitergegeben oder dokumentiert wird? Gibt es genug Zeit dafür?	Art 14 KI-VO, Sorgfaltspflicht
☐	Wie wird mit Halluzinationen, falschen Tatsachen, fehlendem Kontext oder überzeugend klingenden, aber unbelegten Aussagen umgegangen?	Sorgfaltspflichten, § 1299 ABGB KI-Kompetenz (Art 4)

Bias, Diskriminierung und Chancengerechtigkeit

	Frage	Rechtsbezug
☐	Welche Gruppen könnten besonders betroffen sein (Geschlecht, Alter, Behinderung, ethnische Zuschreibung, Sprache, soziale Lage, Familienform, Mehrfachdiskriminierung)?	GlBG, Art 4a KI-VO, Art 27 KI-VO
☐	Welche Unterschiede, stereotype Formulierungen, Darstellungen oder blinde Flecken könnten in der Praxis vorkommen? Welche konkreten Auswirkungen könnte das auf Betroffene haben?	Grundrechte, Vulnerabilität

Transparenz, Grenzen und offene Rechtsfragen

	Frage	Rechtsbezug
☐	Wird Klient*innen, Angehörigen oder anderen Betroffenen erklärt, dass KI im Spiel ist? Falls ja: wann und wie? Falls nein: warum nicht?	Art 50 KI-VO, Art 13, 14 DSGVO, Art 26 Abs 11 KI-VO
☐	Wird KI-generierter Content (Texte, Bilder, Audio) gekennzeichnet, und sind urheberrechtliche Fragen geklärt?	Art 50 KI-VO, UrhG
☐	Was ist in Ihrem Szenario am unklarsten, riskantesten oder unangenehmsten? Wo bestehen noch offene Fragen an die Juristinnen?	Dokumentation, ggf Rechtsberatung

7. Glossar

Begriff	Erklärung
AI Act / KI-VO	Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz
Anbieter	Wer ein KI-System entwickelt (oder entwickeln lässt) und unter eigenem Namen in Verkehr bringt oder in Betrieb nimmt (Art 3 Z 3)
Auftragsverarbeiter	Verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen; benötigt Auftragsverarbeitervereinbarung (Art 28 DSGVO)
Automation Bias	Tendenz, sich übermäßig auf automatisierte Empfehlungen zu verlassen, ohne sie kritisch zu prüfen
Betreiber	Wer ein KI-System in eigener Verantwortung beruflich verwendet (Art 3 Z 4)
Betroffene	Personen, deren Daten verarbeitet werden – in der Sozialen Arbeit vor allem Klient*innen
DSFA	Datenschutz-Folgenabschätzung (Art 35 DSGVO)
GPAI	General Purpose AI: KI-Modell bzw -System mit allgemeinem Verwendungszweck (zB große Sprachmodelle)
GRFA	Grundrechte-Folgenabschätzung (Art 27 KI-VO)
Halluzination	Plausibel klingender, aber faktisch falscher oder erfundener KI-Output
Hochrisiko-KI	KI-System in einem in Anhang I oder III genannten Bereich, das strengen Pflichten unterliegt (Art 6)
Profiling	Automatisierte Verarbeitung personenbezogener Daten zur Bewertung persönlicher Aspekte (Art 4 Z 4 DSGVO; Art 3 Z 52 KI-VO)
Verantwortlicher	Wer über Zwecke und Mittel der Datenverarbeitung entscheidet – idR die Einrichtung
Vulnerabilität	Verletzlichkeit bzw besondere Schutzbedürftigkeit von Personen oder Gruppen

8. Quellen

8.1. Rechtsgrundlagen und Judikatur im Überblick

- Verordnung (EU) 2016/679 (DSGVO), insbesondere Art 4, 6, 9, 22, 28, 35, 82 sowie Erwägungsgründe 26 und 75
- Verordnung (EU) 2024/1689 (KI-Verordnung), insbesondere Art 3, 4, 5, 6, 10, 14, 15, 25, 26, 27, 50, 85, 86, 99 sowie Anhang III
- Richtlinie (EU) 2024/2853 (Produkthaftungsrichtlinie)
- Datenschutzgesetz (DSG), insbesondere § 1 sowie DSFA-Verordnung; Urheberrechtsgesetz (UrhG), insbesondere §§ 1, 10, 15, 42h; ABGB §§ 1295, 1299, 1311, 1313a; Gleichbehandlungsgesetz (GlBG)
- EuGH C-634/21 (SCHUFA, 2023); EuGH C-590/23 (Pastiche, 14.04.2026); OGH 14 Os 95/25i (7.10.2025); EuGH, Brain Products/BioSemi ua, GRUR 2013, 82.
- Europarat: Rahmenübereinkommen über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit (5.9.2024)

8.2. Weiterführende Quellen

- *BfArM*, Orientierungshilfe Medical Apps (Anhaltsbegriffe/-funktionen).
- *Bisset/Dallinger*, KI und Urheberrecht (Stand 7.3.2025, Lexis Briefings in lexis360.at).
- *BMKÖS*, Leitfaden Digitale Verwaltung, Ethik und Recht.
- *Europäische Kommission*, Leitlinien zu den Transparenzpflichten nach Art 50 KI-VO (2026), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10.2026).
- *Europäische Kommission*, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz (2025), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10.2026).
- *Europäische Kommission*, Leitlinien zum Umfang der Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (2025), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10. 2026).
- *Europäische Kommission*, Leitlinien zur Definition eines KI-Systems (2025), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10. 2026).
- *Europäische Kommission*, Entwurf von Leitlinien zur Klassifizierung von Hochrisiko-KI-Systemen nach Art 6 KI-VO (2026), https://digital-strategy.ec.europa.eu/en/library/draft-guidelines-high-risk (abgefragt am 13. 10. 2026).
- *Europäische Kommission*, Verhaltenskodex für KI-Modelle mit allgemeinem Verwendungszweck (2025), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10. 2026).
- *Europäische Kommission*, Verhaltenskodex zur Transparenz KI-generierter Inhalte (2026), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10. 2026).
- *Europäische Kommission*, Vorlage für die Zusammenfassung der Trainingsinhalte von KI-Modellen mit allgemeinem Verwendungszweck (2025), https://digital-strategy.ec.europa.eu (abgefragt am 13. 10. 2026).
- *Fleischmann*, KI-Agenten-Systeme: Einordnung in die KI-Verordnung, RDi 2025, 193.
- *Hense/Mustac*, AI Act kompakt. Compliance, Management & Use Cases in der Unternehmenspraxis (2025).
- *HLEG*, Ethik-Leitlinien für vertrauenswürdige KI (2019).
- *Jahnel/Pallwein-Prettner*, Datenschutzrecht[4] (2025).
- *Mehrabi et al*, A Survey on Bias and Fairness in Machine Learning, ACM Computing Surveys 54 (2021) 115:1.
- *Müller et al*, „AI KNOW" – Information und Mitbestimmung bei KI-basierten Entscheidungen im Beschäftigtenkontext. Theoretischer Bericht (2026).
- *Müller/Scheichenbauer*, KI im Bewerbungsverfahren, ailex 2026, 48.

- *Müller/Scheichenbauer/Schneeberger*, Wissenskultur im KI-Zeitalter – die KI-Kompetenz nach Art 4 AI Act und ihre praktischen Implikationen, ZIIR 2025, 250.
- *Nannini et al*, AI Agents under EU Law, arXiv 2026, 1.
- *Pilgermair,* Datenschutz, in *Loderbaer* (2023), Recht für Sozialberufe.
- *Research Institute,* Aufklärung 4.0 – Entscheidungen der KI als Mensch verstehen. Bericht über die theoretischen Grundlagen des Rechts auf Erläuterung der Entscheidungsfindung im Einzelfall nach Artikel 86 AI Act, Projektbericht (2025).
- *RTR KI-Servicestelle*, Übersichten zu Anbieter- und Betreiberpflichten, https://ki.rtr.at (abgefragt am 13. 10. 2026).
- *Scheichenbauer*, Datenschutz für Vereine (2023).
- *Scheichenbauer*, Praxishandbuch für Datenschutzbeauftragte (2024).
- *Schwenke*, Recht für Online-Marketing und KI (2025).
- *Voigt/Hullen*, Handbuch KI-Verordnung. FAQ zum EU AI Act (2024).
- *Vorberg/Gottberg*, ChatGPT als Medizinprodukt, RDi 2023, 159.
- wiki.atlaws.eu, Hauptseite, https://wiki.atlaws.eu/index.php/Hauptseite (abgefragt am 13. 10. 2026).

Rechtliche Hinweise

Das gegenständliche Informationsmaterial beruht auf der Präsentationsunterlage des Innovationsworkshops Recht (Research Institute – Digital Human Rights Center, 30.06.2026) im Projekt Social AI. Dieses Dokument wurde auf Basis jener Informationen erstellt, die den Autorinnen als für den Zweck des Dokuments relevant erschienen. Die Autorinnen übernehmen jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Dokument enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.

Sofern nicht anders ausgewiesen, wurden die in dem Dokument verwendeten Bildmaterialien mithilfe künstlicher Intelligenz generiert.

Wir dürfen Sie bitten, das geistige Eigentum an dem Dokument im Sinne des Urheberrechts zu respektieren. Auch die Vervielfältigung der Unterlagen und Dateien, die kein veröffentlichtes Werk darstellt, ist nicht gestattet. Ohne schriftliche Genehmigung durch die Autorinnen dürfen weder die Unterlagen selbst noch einzelne Informationen daraus reproduziert oder an Dritte weitergegeben werden.

Kontakt: kontakt@researchinstitute.at



Research Institute – Digital Human Rights Center

© 2026 RI – Alle Rechte vorbehalten