Bundesministerium
Arbeit, Soziales, Gesundheit,
Pflege und Konsumentenschutz

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

**Research Institute – Digital Human Rights Center**

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

Wien, 28. Februar 2025


| | |
|---|---|
| Projektleitung: | Madeleine Müller |
| | Christof Tschohl |
| Autor:innen: | Jan Hospes |
| | Madeleine Müller |
| | Philipp Poindl |
| | Robert Rothmann |
| | Heidi Scheichenbauer |
| | David M. Schneeberger |
| Grafische Gestaltung: | Andreas Czák |



Konsolidierter Bericht zu den rechtlichen, sozialwissenschaftlichen und ethischen Grundlagen des Rechts auf Erläuterung der Entscheidungsfindung im Einzelfall nach Artikel 86 AI Act in Zusammenschau mit den relevanten Bestimmungen der DSGVO im Rahmen des Projekts „Aufklärung 4.0 – Entscheidungen der KI als Mensch verstehen“, das vom Research Institute – Digital Human Rights Center im Auftrag des Bundesministeriums für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz durchgeführt wurde.

**IMPRESSUM**

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

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

Web: https://researchinstitute.at

E-Mail: mailto:office@researchinstitute.at

Mastodon: mastodon.researchinstitute.at/@researchinstitute

© 2025 RI – Alle Rechte vorbehalten

---

**Gendergerechte Sprache**

Die relevanten Gesetzestexte verwenden für die Beschreibung privater und juristischer Personen das generische Maskulinum. Die im Gesetz definierten Begriffe (zB der Verantwortliche) werden im vorliegenden Bericht daher direkt aus dem Gesetzestext übernommen. In allen anderen Fällen wird im Sinne eines diskriminierungsfreien Sprachgebrauchs der Gender-Doppelpunkt (:) verwendet.

# 1 Inhaltsverzeichnis


**1 Inhaltsverzeichnis ... 4**

**2 Management Summary ... 7**

**3 Projekt „Aufklärung 4.0 – Entscheidungen der KI als Mensch verstehen“ ... 8**

**3.1 Projekthintergrund ... 8**

**3.2 Methodisches Vorgehen in der Projektentwicklung ... 10**

**3.3 Einbindung von Stakeholdern ... 11**

**4 Einleitung ... 12**

**5 Das Recht auf Erklärung in der rechtlichen Analyse ... 15**

**5.1 Einleitung ... 15**

**5.2 Rechtlicher Rahmen ... 16**

5.2.1 Datenschutz-Grundverordnung (DSGVO) ... 16

5.2.2 AI Act ... 22

5.2.2.1 Einleitung ... 22

5.2.2.2 Anwendungsbereich ... 22

5.2.2.3 Verbotene Praktiken ... 25

5.2.2.4 Hochrisiko-KI-Systeme ... 26

5.2.2.5 Anforderungen an Hochrisiko-KI-Systeme ... 29

**5.3 Praxisbeispiele und rechtliche Einordnung in den Anwendungsbereich ... 32**

5.3.1 Preisbildung Lebens- und Krankenversicherung (Use Case 1) ... 32

5.3.1.1 Allgemeines ... 32

5.3.1.2 Rechtliche Beurteilung ... 33

5.3.2 Churn Predictions (Use Case 2) ... 33

5.3.2.1 Beispielhafter Ablauf Scoring ... 34

5.3.2.2 Beispielhafter Ablauf Anwendung ... 35

5.3.2.3 Rechtliche Beurteilung ... 35

5.3.3 Bonitätsprüfungen (Use Case 3) ... 37

5.3.3.1 Beispielhafter Ablauf der Bonitätsprüfung ... 37

5.3.3.2 Rechtliche Beurteilung ....38
5.3.4 Emotionserkennung im Marketing bzw zur Absatzförderung (Use Case 4) ....39
5.3.4.1 Datenbasis und Einordnung gemäß DSGVO und AI Act ....40
5.3.4.2 Biometrischer Daten gem AI Act auch maßgeblich für DSGVO? ....41
5.3.4.3 Biometrischer Daten gem DSGVO auch maßgeblich für AI Act? ....42
5.3.4.4 Fazit zu Begrifflichkeiten biometrischer Daten ....43
5.3.4.5 Einordnung von Emotionserkennungssystemen gem AI Act ....45
5.3.4.6 Rechtliche Beurteilung ....46

**5.4 Relevante Bestimmungen der Datenschutz-Grundverordnung (DSGVO) ....52**
5.4.1 Artikel 22 DSGVO ....52
5.4.1.1 Allgemeines ....53
5.4.1.2 „Entscheidung“ ....55
5.4.1.3 „Rechtliche Wirkung“ ....56
5.4.1.4 Der Ausdruck „sie in ähnlicher Weise erheblich beeinträchtigt“ ....58
5.4.1.5 Ausnahmen vom Verbot der automatisierten Entscheidungsfindung ....60
5.4.2 Artikel 15 Abs 1 lit h DSGVO ....64
5.4.2.1 Einleitung ....64
5.4.2.2 Involvierte Logik ....65
5.4.2.3 Tragweite und angestrebte Auswirkungen ....71
5.4.3 Informationspflichten nach der DSGVO ....73
5.4.3.1 Artikel 13 DSGVO ....74
5.4.3.2 Artikel 14 DSGVO ....75
5.4.3.3 Zusammenschau der Art 13 und 14 DSGVO ....77

**5.5 Das Recht auf Erklärung im AI Act ....79**
5.5.1 Anwendungsbereich des Artikel 86 AI Act ....79
5.5.2 Bestandteile der Erklärung ....88
5.5.2.1 Rolle des KI-Systems an der Entscheidungsfindung ....88
5.5.2.2 Die wichtigsten Elemente der getroffenen Entscheidung ....88
5.5.3 Formale Aspekte im Zusammenhang mit Art 86 AI Act ....94
5.5.3.1 Frist ....94
5.5.3.2 Form und Kosten der Erklärung ....94
5.5.3.3 Negativauskunft ....95
5.5.4 Zur Relevanz von Art 86 AI Act ....95
5.5.5 Abgrenzungsfragen – „Lückenfüller“ Art 86 AI Act? ....96

5.5.6 Herausforderungen bei der Umsetzung ..... 99
5.5.7 Informationspflichten gem AI Act ..... 100

**5.6 Sanktionen und Schadenersatz ..... 105**

**5.7 Vergleich und Subsumtion der Praxisbeispiele ..... 109**

5.7.1 Relevante Bestimmungen der DSGVO ..... 110
5.7.2 Art 86 AI Act und damit zusammenhängende Bestimmungen ..... 112
5.7.3 Zusammenfassende Tabelle zur Einordnung der Fallbeispiele ..... 116

**6 Sozialwissenschaftliche Aspekte ..... 118**

**6.1 Auskunft ..... 118**

**6.2 Automation Bias ..... 122**

**7 Ethische Aspekte ..... 126**

**8 Conclusio ..... 130**

**9 Anhang ..... 132**

**9.1 Hochrisiko-KI-Systeme gem Anhang III AI Act ..... 132**

**9.2 Abkürzungsverzeichnis ..... 136**

# 2 Management Summary

Der vorliegende Grundlagenbericht zum Projekt „Aufklärung 4.0 - Entscheidungen der KI als Mensch verstehen“, welches vom Research Institute - Digital Human Rights Center im Auftrag des Ministeriums für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz durchgeführt wird, dokumentiert die rechtlichen Grundlagen des Rechts auf Erklärung, wie es in der Verordnung des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz („KI-Verordnung“ oder „AI Act“[1]) mit Art 86 normiert ist. Zusätzlich bezieht der Bericht auch damit zusammenhängende sozialwissenschaftliche und ethische Überlegungen mit ein, um ein breiteres Bild von diesem Betroffenenrecht zu gewinnen. Der Fokus des Berichts liegt auf der Schaffung von Synergien von bereits bestehenden datenschutzrechtlichen Regelungen, insbesondere jene der Datenschutz-Grundverordnung (DSGVO)[2], mit dem Recht auf Erläuterung der Entscheidungsfindung im Einzelfall gem Art 86 AI Act (fortan der Einfachheit halber als „Recht auf Erklärung“ bezeichnet). Des Weiteren beinhaltet er eine umfassende Literatur- und Judikaturrecherche zu diesem Betroffenenrecht im Zusammenspiel mit ausgewählten Fallbeispielen („Use Cases“) zur Herstellung des Praxisbezugs, der wiederum theoretisch gründlich fundiert ist.

In Zusammenschau der genannten Aspekte dient der gegenständliche Bericht als theoretische Grundlage für zwei Leitfäden für den Umgang mit dem Recht auf Erklärung in der Praxis, die im Rahmen des Projekts ebenfalls erarbeitet wurden. Ein Leitfaden fokussiert dabei die Betroffenen- bzw Konsument:innenperspektive, da Konsument:innen zu den Hauptadressaten des Auskunftsanspruchs nach Art 86 AI Act gehören. Andererseits ist es zugleich unerlässlich, die Perspektive von Unternehmen und sonstigen Einrichtungen einzunehmen, da diese genau jene Stellen darstellen, die im Umgang mit Betroffenenrechten besonders geschult werden müssen. Es sind dabei insbesondere die Mitarbeiter:innen dieser Einrichtungen, die mit Ansprüchen von Betroffenen konfrontiert werden und oftmals nicht genau wissen, wie sie diesen angemessen nachzukommen haben. Dies insbesondere in Bezug auf neue rechtliche Vorschriften, für die noch keine konkreten Leitlinien bestehen, weshalb der zweite Leitfaden an diese Zielgruppe gerichtet ist. Um die praktische Relevanz der Leitfäden zu gewährleisten und die praktische Durchsetzbarkeit des Rechts auf Erklärung zu verbessern, wurden im Rahmen des Projekts Stakeholder-Workshops abgehalten, um sowohl die Konsument:innen-Perspektive als auch jene von Unternehmen und sonstigen Einrichtungen miteinzubeziehen.

[1] 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) 300/2008, (EU) 167/2013, (EU) 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 (AI Act/KI-VO), ABl L 2024/144, 1.

[2] 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), ABl L 2016/119, 1.

# 3 Projekt „Aufklärung 4.0 – Entscheidungen der KI als Mensch verstehen“

## 3.1 Projekthintergrund

Die Verordnung des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz („KI-Verordnung“ oder „AI Act“) wurde am 12. Juli 2024 offiziell im Amtsblatt der Europäischen Union veröffentlicht und ist mit August 2024 in Kraft getreten. Der AI Act verfolgt einen risikobasierten Ansatz, der KI-Systeme je nach Art, Einsatzgebiet und potenziellen Risiken für die Sicherheit, Gesundheit und Grundrechte betroffener Personen in verschiedene Risikoklassen einteilt, an die wiederum unterschiedliche Verpflichtungen und Rechtsfolgen geknüpft sind.[3] Je nach Risikoeinstufung bzw KI-System sind die Vorschriften innerhalb von 6 bis 36 Monaten nach dem Inkrafttreten anwendbar.

Dies bedeutet für unzählige Unternehmen und sonstige Einrichtungen eine maßgebliche Umstellung sowie die Integration eines breiten Normenkatalogs in deren Tätigkeiten. Dies insbesondere im Hinblick auf den Umgang mit Betroffenenrechten, da vielen im Geschäftsalltag eingesetzten KI-basierten Systemen oftmals ein betroffenes Individuum gegenübersteht, das mit besagtem System in Berührung kommt. Ein breiter Anwendungsfall sind KI-basierte Systeme, auf Basis deren Ausgaben Entscheidungen getroffen werden, welche wiederum Einzelpersonen oder Personengruppen betreffen. Beispiele, in denen bestimmte Personen(gruppen) der Entscheidung eines KI-basierten Systems unterliegen können, finden sich etwa im Bereich der Kreditwürdigkeitsprüfung sowie auch beim Abschluss von Kranken- und Lebensversicherungen (Vgl hierzu Anhang III Punkt 5 AI Act, demgemäß derartige Systeme als „Hochrisiko-KI-Systeme“ eingestuft werden). Ein anderer Fall, der gem Anhang III Punkt 5 AI Act ebenfalls als hochriskant gilt, betrifft den Einsatz von KI-basierten Systemen zur Beurteilung, ob natürliche Personen Anspruch auf öffentliche Dienste und Leistungen haben. Die Liste ließe sich um eine Vielzahl an Anwendungsfällen erweitern und verdeutlicht, wie häufig natürliche Personen und Personengruppen in Zukunft Entscheidungen von KI-basierten Systemen unterliegen werden, die als hochriskant eingestuft sind, bzw bereits davon betroffen sind.

Art 86 AI Act sieht ein „Recht auf Erläuterung der Entscheidungsfindung im Einzelfall“ vor, wonach von einer Hochrisiko-KI-gestützten Entscheidung betroffenen Personen ein Auskunftsanspruch in Bezug auf die wesentlichen Elemente der getroffenen Entscheidung sowie auf die Rolle des KI-Systems im Entscheidungsprozess zukommt (im Folgenden: „Recht auf Erklärung“). Eine detaillierte Handlungsanweisung, wie Unternehmen diesem Anspruch in der Praxis nachzukommen haben bzw welche konkreten Informationen die Auskunftserteilung beinhalten muss, bleibt Art 86 AI Act allerdings schuldig. Rechtsprechung zu Art 86 AI Act

[3] Vgl *Metikos/Ausloos*, The Right to an Explanation in Practice. Insights from Case Law for the GDPR and the AI Act, Law, Innovation, and Technology 2025, iE, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4996173 17.2 2025 (Stand 24. 10. 2024).

besteht (naturgemäß) noch nicht, wobei ein erstes Vorabentscheidungsersuchen eingereicht wurde.[4] Dabei ist es jedoch von immenser Bedeutung, dass Unternehmen und Vereine, insbesondere aber auch öffentliche Einrichtungen, im Sinne der Compliance mit den Prinzipien der Transparenz und Rechenschaftspflicht diesem Betroffenenrecht in geeigneter Weise nachkommen.

Neben den rechtlichen Verpflichtungen, die der AI Act den jeweiligen Stellen auferlegt, hat auch das Erfordernis der Einhaltung von ethischen Prinzipien in die Debatte um Künstliche Intelligenz Einzug gefunden und sich zu einem zentralen Eckpfeiler der österreichischen KI-Strategie entwickelt. An diesem Punkt setzt das Projekt an mit dem Ziel, konkrete Leitlinien für den Umgang mit dem Recht auf Erklärung zu entwickeln und damit den hohen rechtlichen sowie ethischen Maßstäben angemessen Rechnung zu tragen, zu denen sich Österreich in seiner nationalen KI-Strategie bekannt hat. Entsprechend eines am Gemeinwohl orientierten und auf Basis von Grund- und Menschenrechten entwickelten Ansatzes soll das Vertrauen in den Einsatz von Künstlicher Intelligenz gestärkt und ein verantwortungsvoller Umgang mit dieser gewährleistet werden.

Das Recht auf Erklärung gilt dabei als zentrale Säule zur Verwirklichung dieses Ansatzes, da dieser Auskunftsanspruch für Betroffene oftmals die Voraussetzung darstellt, um auf Basis dieser Informationen bestimmte Ansprüche wie etwa Schadenersatz geltend machen bzw den Rechtsweg beschreiten zu können. Die Entwicklung von konkreten Leitlinien zu Art 86 AI Act stellt somit die Basis dar, um nicht nur Transparenz und Rechenschaftspflicht zu gewährleisten, sondern in weiterer Konsequenz auch dem Rechtsstaatsprinzip zu entsprechen und demokratische Werte zu stärken. Zentral ist dabei die Schaffung einer für alle Menschen verständlichen und leicht zugänglichen Basis, mit der das Verständnis der Funktionsweise von Künstlicher Intelligenz gestärkt wird.

[4] Vorabentscheidungsersuchen EuGH 25. 11. 2024, C-806/24, *Yettel Bulgaria*, ECLI noch nicht zugewiesen.

## 3.2 Methodisches Vorgehen in der Projektentwicklung

Der gegenständliche Grundlagenbericht ist Teil eines Pakets von mehreren Dokumenten, die im Rahmen des Projekts „Aufklärung 4.0 – Entscheidungen der KI als Mensch verstehen“ verfasst wurden.

Der Projektablauf gliederte sich dazu in unterschiedliche Phasen mit jeweils unterschiedlichen Zielsetzungen (siehe Abbildung 1). Zunächst wurde der vorliegende Grundlagenbericht erarbeitet, der eine fundierte Aufarbeitung des Rechts auf Erklärung nach Art 86 AI Act beinhaltet. Da sich die Regelungen zur Entscheidungsfindung mittels KI-basierten Systemen teilweise mit bereits bestehenden Bestimmungen, wie etwa Art 22 DSGVO zu automatisierten Entscheidungen im Einzelfall und dem damit korrespondierenden Auskunftsanspruch nach Art 15 Abs 1 lit h DSGVO, decken, wurden Synergien mit den bestehenden datenschutzrechtlichen Regelungen geschaffen und in der Erarbeitung des gegenständlichen Berichts darauf aufgebaut. Diese wurden unter Heranziehung relevanter Literatur und aktueller Rechtsprechung um neue Handlungsanweisungen erweitert, damit sie als eine Art „Handbuch“ für verschiedenste Stellen, Mitarbeiter:innen und Betroffene gleichermaßen, fungieren können und verständlich wiedergeben, wen welche Pflichten treffen bzw wem welche Rechte zustehen. Um bereits so früh wie möglich einen Praxisbezug herzustellen, wurden konkrete Praxisbeispiele ausgewählt, um die teils abstrakten rechtlichen Überlegungen verständlich und praxisnah zu veranschaulichen. Die rechtliche Analyse wurde um eine sozialwissenschaftliche sowie ethische Betrachtung ergänzt, um ein breiteres Bild von der Relevanz des Rechts auf Erklärung in der Praxis zu zeichnen.

Darauf aufbauend wurden einerseits Leitlinien mit konkreten Orientierungshilfen für Unternehmen entwickelt, damit diese im Umgang mit dem Auskunftsanspruch von Betroffenen nach Art 86 AI Act geschult werden und auf niederschwellige Handlungsanweisungen zurückgreifen können. Ein weiterer Leitfaden wurde für Konsument:innen und ihre Interessenvertretungen erarbeitet, damit diese darüber Kenntnis erlangen, worüber sie Auskunft verlangen können, welche Fragen sie stellen können und welche Möglichkeiten im Falle mangelhafter Auskünfte in der Folge offenstehen.[5]

Um sowohl die Perspektive von betroffenen Unternehmenssektoren als auch Konsument:innen bestmöglich abbilden zu können, beinhaltete das Projekt einen ausgedehnten Stakeholder-Prozess, in dessen Rahmen mehrere Workshops abgehalten wurden, deren Ergebnisse wiederum in die beschriebenen Schlüsseldokumente eingearbeitet wurden. Die Projektlaufzeit erstreckte sich von Juni 2024 bis April 2025 und schließt mit der Präsentation des Grundlagenberichts und der beiden Leitfäden sowie mit einer Pilotschulung im Umgang mit diesen.

[5] Beide Leitfäden sowie der Endbericht können auf der Webseite des Sozialministeriums, auf der aktuelle Studien und Berichte aus dem Bereich Konsumentenpolitik veröffentlicht werden, abgerufen werden.

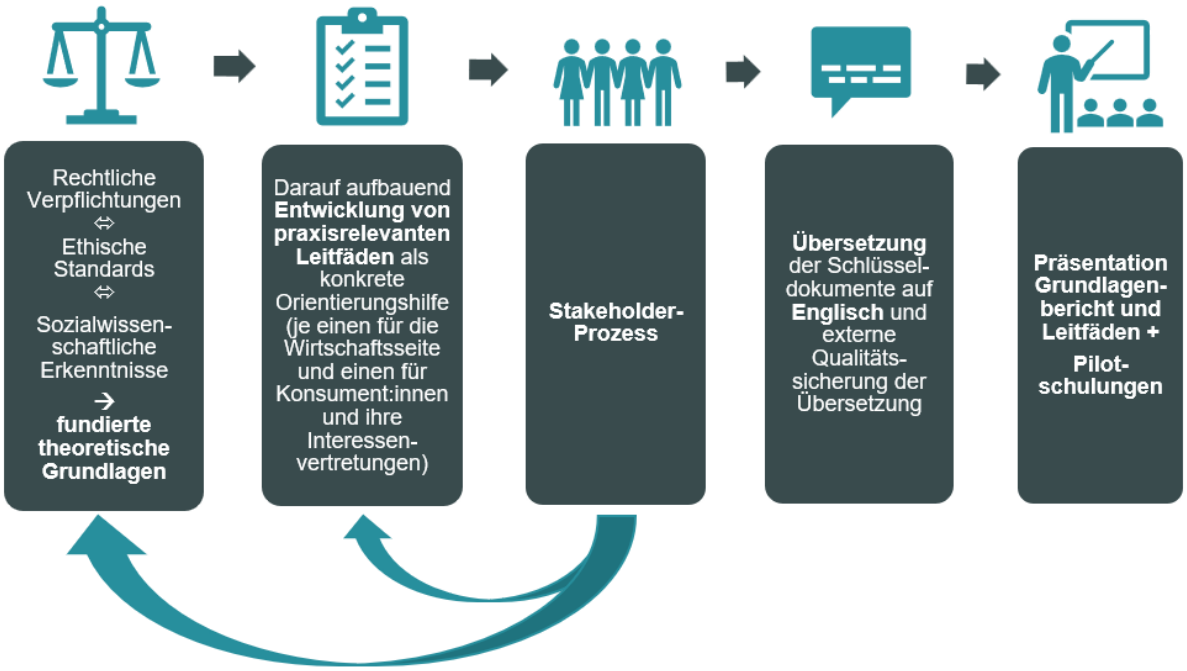


Abbildung 1: Organisatorische Schritte des Projektablaufs

## 3.3 Einbindung von Stakeholdern

Um die praktische Relevanz des Grundlagenberichts und der Leitfäden zu gewährleisten, bildete der Stakeholder-Prozess einen zentralen Bestandteil des Projekts, wobei sowohl Interessenvertretungen der Wirtschaftsseite als auch der Konsument:innenseite beteiligt waren. Im Rahmen des Projekts wurden mehrere Stakeholderworkshops abgehalten, um sowohl die Perspektive von Konsument:innen als auch jene von Unternehmen und sonstigen Einrichtungen miteinzubeziehen und damit die praktische Durchsetzbarkeit des Rechts auf Erklärung zu verbessern. Die Perspektive der Stakeholder lieferte dabei nicht nur entscheidende Erkenntnisse für die theoretischen Grundlagen, sondern stellte auch einen wertvollen Input in der Formulierung der Praxisbeispiele („Use Cases“) sowie zur Struktur und Ausgestaltung der Leitfäden dar.

Insgesamt wurden zwischen September 2024 und November 2024 drei Workshops zur Einbindung relevanter Stakeholder abgehalten, in deren Rahmen Sichtweisen, Herausforderungen und Interpretationen geteilt sowie praktische Fragen zur Diskussion gestellt wurden.

# 4 Einleitung

Das Recht auf Erklärung einer Entscheidung als Betroffenenrecht bzw die damit korrespondierende Begründungspflicht durch Entscheidungsträger:innen hat die Funktion, die Rechtmäßigkeit von Entscheidungen überprüfbar zu machen und Betroffenen die Möglichkeit zu geben, ausreichende Informationen über eine sie betreffende Entscheidung zu erhalten sowie ihre Rechte zu schützen. Das Recht auf Erklärung stellt außerdem eine wichtige Prämisse für die Ausübung weiterer Betroffenenrechte dar, wie am Beispiel der DSGVO veranschaulicht werden kann: Art 15 DSGVO regelt das Auskunftsrecht von Personen, deren personenbezogene Daten verarbeitet werden. Das Recht auf Auskunft zählt zu den am häufigsten wahrgenommenen Betroffenenrechten der DSGVO und fungiert als „Türöffner" für die Ausübung anderer Betroffenenrechte, beispielsweise das Recht auf Löschung und auf Berichtigung von Daten.[6]

Im Zeitalter des vermehrten Einsatzes KI-basierter Systeme in Entscheidungsprozessen gilt es, das Recht auf Erklärung neu zu denken und damit zusammenhängende Herausforderungen im Sinne der Betroffenen zu thematisieren. Denn KI-basierte Systeme operieren oft in einer Weise, die für Menschen schwierig zu verstehen ist, und bedienen sich undurchsichtiger Mechanismen, weshalb verständliche Erläuterungen zum Hintergrund bestimmter Ergebnisse oft fehlen.[7] Diese sog „Black-Box-Problematik" verdeutlicht die Notwendigkeit, KI-gestützte Entscheidungen transparenter zu gestalten, was zum Entstehen eines ganzen Teilbereichs der Forschung, „eXplainable AI" (kurz: XAI) oder „erklärbare KI", geführt hat. Selbst wenn es bisher keine einheitliche Definition von XAI gibt, umfasst dieser Bereich grundsätzlich zwei Dimensionen: Einerseits bezeichnet XAI die Entwicklung von White-/Glass-Box bzw ante-hoc-interpretierbaren Modellen, die generische (globale) Erklärungen über Mechanismen liefern und dadurch in ihrer Gesamtheit, losgelöst von einer Einzelentscheidung, interpretiert werden können.[8] Andererseits versteht man darunter den Fokus auf KI-Systeme, die nicht nur präzise Vorhersagen oder Entscheidungen treffen, sondern auch (lokale) Erklärungen darüber liefern können, wie eine spezifische Entscheidung oder Schlussfolgerung in einem bestimmten Fall zustande gekommen ist (sog post-hoc-Interpretierbarkeit).[9] Dies impliziert, dass XAI in der Lage sein sollte, die von ihr durchgeführten Operationen zu erläutern, die nächsten Schritte zu prognostizieren und die verwendeten Informationsquellen zur Entscheidungsfindung offenzulegen, damit Nutzer:innen die Gründe für eine automatisierte Entscheidung verstehen können.[10]

---

[6] Vgl *Datenschutzkonferenz*, Deutsche Datenschutzaufsichtsbehörden beteiligen sich an CEF 2024. Beginn der koordinierten Aktion zum Auskunftsrecht, https://datenschutzkonferenz-online.de/media/pm/2024-02-28_DSK-PM_CEF-2024-Auskunftsrecht.pdf (abgefragt am 14. 2. 2025).

[7] Vgl *Winikoff/Sardelic*, Artificial Intelligence and the Right to Explanation as a Human Right, IEEE Internet Computing 2021, 108 (108).

[8] Vgl *Winikoff/Sardelic*, IEEE Internet Computing 2021, 108 (108).

[9] Vgl *Cervera Navas*, Explainable Artificial Intelligence needs Human Intelligence, https://www.edps.europa.eu/press-publications/press-news/blog/explainable-artificial-intelligence-needs-human-intelligence_en (Stand 2. 6. 2023).

[10] Vgl *Cervera Navas*, Explainable Artificial Intelligence needs Human Intelligence, https://www.edps.europa.eu/press-publications/press-news/blog/explainable-artificial-intelligence-needs-human-intelligence_en (Stand 2. 6. 2023).

In beiden Bereichen existieren dutzende von verschiedenen Modellen (lineare/logistische Regression, Entscheidungsbäume) bzw Techniken wie das Hervorheben der wichtigsten Merkmale (zB farbige Kennzeichnung der wichtigsten Pixel bei Bilderkennung) (feature-importance/feature-salience), das Geben von Beispielen bzw Informationen dazu, welche Merkmale sich minimal ändern müssten, um den Ausgang der Entscheidung zu ändern (counterfactuals) oder seit Verbreitung von Large Language Models auch zunehmend Erklärungen in natürlicher Sprache.[11]

XAI und die Erklärbarkeit von Entscheidungen werden weithin als wesentlicher Bestandteil von Transparenz erachtet, welche wiederum das Vertrauen in KI-basierte Systeme stützt.[12] Die Pflicht, Entscheidungen zu erklären, ist dabei ein häufiges Element, um Accountability bzw Rechenschaft herzustellen.[13] Aus diesem Grund wurde das Recht auf Erklärung in den AI Act aufgenommen und mit Art 86 in der finalen Fassung des Regelwerks als Recht auf Erläuterung der Entscheidungsfindung im Einzelfall in Form eines Betroffenenrechts verankert. Art 86 AI Act gesteht Personen, die von einer Entscheidung betroffen sind, die der Betreiber auf der Grundlage der Ausgaben von bestimmten Hochrisiko-KI-Systemen getroffen hat, das Recht zu, eine klare und aussagekräftige Erläuterung zur Rolle des Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten. Damit zielt der AI Act darauf ab, betroffenen Personen, welche sich ohnehin gegenüber KI einsetzenden Einrichtungen in einer vulnerablen Position befinden, da sie keinen Einblick in deren KI-basierte Prozesse und die Komplexität dieser Mechanismen haben, einen weitergehenden Schutz zuzugestehen sowie das dadurch bestehende Machtungleichgewicht zwischen den involvierten Parteien zumindest etwas auszugleichen.[14] Darüber hinaus erlaubt es die Erläuterung einer KI-gestützten Entscheidung der betroffenen Person, die Entscheidung rechtlich anzufechten, bietet Entwickler:innen Einblick in mögliche negative Nebeneffekte des Systems und trägt generell zur Erhöhung der Legitimität der Entscheidung bei.[15] Eine genaue Anleitung, welche Informationen die Erklärung enthalten muss und in welcher Form sie auszugestalten ist, bleibt Art 86 AI Act jedoch schuldig, weshalb im Folgenden eine rechtliche Analyse dieser Bestimmung und ihrer wesentlichen Inhalte in Zusammenschau mit den relevanten datenschutzrechtlichen Bestimmungen erfolgt. Dazu wird zunächst der rechtliche Hintergrund der einschlägigen Rechtsrahmen - nämlich jener der DSGVO und jener des AI Act - erläutert und deren Relevanz für das gegenständliche Projekt aufgezeigt. Im Anschluss erfolgt eine Sachverhaltsdarstellung der ausgewählten Praxisbeispiele ("Use Cases"), die im Rahmen der Stakeholder-Workshops konkretisiert und näher ausformuliert wurden. Folgende Use Cases stehen dabei im Fokus:

---

[11] Weiterführend *Molnar*, Interpretable Machine Learning. A Guide for Making Black Box Models Explainable², https://christophm.github.io/interpretable-ml-book/ (Stand 31. 7. 2024).

[12] Vgl etwa *AI HLEG*, Ethik-Leitlinien für eine vertrauenswürdige KI (2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425.

[13] *Yeung/Ranchordas*, An Introduction to Law and Regulation. Text and Materials² (2024) 372 f.

[14] Vgl *Dirutigliano*, Some considerations on the relationship between the right to a reasoned decision and the right to explanation in the proposal of the Artificial Intelligence Act, https://digi-con.org/some-considerations-on-the-relationship-between-the-right-to-a-reasoned-decision-and-the-right-to-explanation-in-the-proposal-of-the-artificial-intelligence-act/ (Stand 4. 10. 2023).

[15] Vgl *Asghari/Birner/Burchardt/Dicks/Faßbender/Feldhus/Hewett/Hofmann/Kettemann/Schulz/Simon/Stolberg-Larsen/Züger*, What to explain when explaining is difficult? An interdisciplinary primer on XAI and meaningful information in automated decision-making (2022) 1, https://graphite.page/explainable-ai-report/.

1. Preisbildung in der Lebens- und Krankenversicherung (Use Case 1)
2. KI-basierte Vorhersagen von Kundenabwanderungen, sog „Churn Predictions“ (Use Case 2)
3. Bonitäts- und Kreditwürdigkeitsprüfung (Use Case 3)
4. Emotionserkennung im Marketing bzw zur Absatzförderung (Use Case 4)

Anschließend werden die einschlägigen datenschutzrechtlichen Bestimmungen erläutert. Den Kern des gegenständlichen Berichts bildet die Analyse des Rechts auf Erklärung nach Art 86 AI Act, dessen wesentliche Inhalte herausgearbeitet werden und welches anhand der ausgewählten Praxisbeispiele veranschaulicht wird. Abschließend werden in Ergänzung sozialwissenschaftliche sowie ethische Aspekte des Rechts auf Erklärung aufgezeigt, um ein über das Recht hinausgehendes Bild von sowohl den Rechten von betroffenen Personen nach Art 86 AI Act als auch von den damit korrespondierenden Pflichten von Einrichtungen, die sich KI-basierten Systemen zur Entscheidungsfindung bedienen, zu zeichnen.

# 5 Das Recht auf Erklärung in der rechtlichen Analyse

## 5.1 Einleitung

Das Recht auf Erklärung in Bezug auf automatisierte bzw KI-gestützte Entscheidungsfindungen im Einzelfall gem Art 86 AI Act ist kein Novum. Die DSGVO enthält bereits Regelungen zur automatisierten Entscheidungsfindung und normiert ein damit korrespondierendes Auskunftsrecht. Art 22 DSGVO legt fest, dass Personen das Recht haben, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, außer, es sind gewisse Voraussetzungen erfüllt. Der generelle Auskunftsanspruch nach Art 15 DSGVO normiert in Abs 1 lit h ein damit korrespondierendes Recht auf Erklärung, wonach betroffenen Personen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu beauskunften sind.

Der potenzielle Anwendungsbereich des Art 22 DSGVO (iVm Art 15 Abs 1 lit h DSGVO) für eine Vielzahl von KI-Systemen wirft die Frage nach dem Zusammenspiel dieser Bestimmung(en) mit Art 86 AI Act auf.[16] Denn grundsätzlich tritt der AI Act neben die DSGVO und lässt den Geltungsgehalt der DSGVO unberührt, während in anderen Bereichen Überschneidungen der beiden Verordnungen entstehen können.[17] In Bezug auf das Recht auf Erklärung könnte dies der Fall sein, sofern ein KI-System unter bestimmten Voraussetzungen personenbezogene Daten iSd Art 4 Abs 1 DSGVO verarbeitet und eine vollautomatisierte Entscheidung iSd Art 22 DSGVO trifft, wodurch sowohl der Anwendungsbereich der DSGVO als auch jener des AI Act eröffnet ist.[18] Als Beispiel wäre ein KI-System zur Bonitätsprüfung zu nennen, das auf Basis von bestimmten Merkmalen einer Person – wie Alter, Geschlecht, Familienstand, Meldeadresse, etc. – einen „Credit Score“ vergibt, aufgrund dessen über die Gewährung eines Kredits an diese Person entschieden wird.[19]

Es zeigt sich somit eine enge Verknüpfung zwischen den Bestimmungen der DSGVO und des AI Act in Bezug auf algorithmische Entscheidungsfindung und das Recht auf Erklärung, weshalb im gegenständlichen Kapitel der rechtliche Rahmen dieser Normen analysiert und deren Zusammenspiel bewertet wird. Ebenso sollen die nachfolgenden Ausführungen Aufschluss darüber geben, inwieweit sich Elemente des Auskunftsanspruchs nach Art 15 Abs 1 lit h DSGVO in Art 86 AI Act finden und welche Ableitungen sich aus der bisherigen Literatur und Judikatur zum Recht auf Erklärung in der DSGVO auf den AI Act übertragen lassen.

[16] Vgl *Paal/Hüger,* Die KI-VO und das Recht auf menschliche Entscheidung, MMR 2024, 540 (542).
[17] Vgl *Paal/Hüger,* MMR 2024, 540 (542).
[18] Vgl *Paal/Hüger,* MMR 2024, 540 (542).
[19] Vgl in diesem Fall die Entscheidung des EuGH zur deutschen Kreditauskunftei SCHUFA: EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957.

## 5.2 Rechtlicher Rahmen

### 5.2.1 Datenschutz-Grundverordnung (DSGVO)

Die im Jahr 2016 vom EU-Gesetzgeber verabschiedete DSGVO ist seit Mai 2018 direkt anwendbar und verfolgt das Ziel, die Fragmentierung des Datenschutzes innerhalb der EU-Mitgliedstaaten und die daraus resultierenden Rechtsunsicherheiten zu beseitigen.[20] Damit ist die DSGVO Teil einer umfassenden Konzeption der EU zur Digitalisierung von Gesellschaft und Wirtschaft, wobei gleichzeitig die Freiheiten und Grundrechte der Menschen, die Demokratie und Rechtsstaatlichkeit angesichts des digitalen Wandels gewahrt werden sollen sowie gewährleistet werden soll, dass natürliche Personen die Kontrolle über ihre eigenen Daten behalten.[21] Zentraler Bestandteil der DSGVO ist der Schutz personenbezogener Daten bei gleichzeitiger Gewährleistung des freien Datenverkehrs[22], womit dieser Rechtsakt eine wesentliche Erkenntnisquelle für die Auslegung der in der GRC gewährleisteten Grundrechte, insb Art 8, darstellt.[23] Die DSGVO verfolgt einerseits das sog Marktortprinzip, wonach europäische Konsument:innen und Betroffene durch das Regelwerk geschützt werden, unabhängig davon, wo die eigentliche Datenverarbeitung stattfindet.[24] Zusätzlich gilt gem Art 3 Abs 1 das Niederlassungsprinzip, wonach die DSGVO auf Datenverarbeitungen Anwendung findet, die im Rahmen der europäischen Niederlassung eines Unternehmens oder einer sonstigen Einrichtung stattfinden.[25] Wesentliche Elemente der DSGVO sind weiters die Verbesserung der Transparenz für Betroffene sowie die Gewährleistung des technischen Datenschutzes durch die Verankerung der Prinzipien des Datenschutzes durch Technikgestaltung („privacy-by-design“) und Datenschutz durch datenschutzfreundliche Voreinstellung („privacy-by-default“). Die DSGVO verfolgt darüber hinaus einen risikobasierten Ansatz, wonach vor bestimmten risikoreichen Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen ist (Vgl Art 35 DSGVO).[26] Die DSGVO enthält weiters einen Katalog an Betroffenenrechten, wozu etwa das Recht auf Auskunft (Art 15), auf Berichtigung von Daten (Art 16), auf Löschung von Daten (Art 17), auf Einschränkung der Verarbeitung (Art 18) sowie umfassende Informationspflichten (Art 13 und 14) zählen.

Sachlich bezieht sich die DSGVO auf den Schutz von personenbezogenen Daten bei deren Verarbeitung.[27] Darunter versteht die DSGVO gem Art 4 Z 1 „[...] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ beziehen. Identifiziert ist eine Person, wenn die Datenverwender:innen die jeweilige Person identifizieren können, etwa mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten

[20] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch² (2024) 2.
[21] Vgl *Köllmann*, Implementierung elektronischer Überwachungseinrichtungen durch Betriebsvereinbarungen vor dem Hintergrund der DSGVO (2021) 184; *Weichert* in *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG. Kompaktkommentar³ (2024) Einleitung Rz 24.
[22] Vgl auch die Ziele der DSGVO in Art 1.
[23] MwN *Weichert* in *Däubler et al,* EU-DSGVO³ Einleitung Rz 24.
[24] Zum räumlichen Anwendungsbereich der DSGVO vgl Art 3.
[25] Vgl *Köllmann*, Implementierung 197.
[26] *Weichert* in *Däubler et al,* EU-DSGVO³ Einleitung Rz 27 ff.
[27] *Scheichenbauer*, Datenschutz für Vereine² (2023) 1.

oder zu einer Online-Kennung.[28] Als identifizierbar wird eine Person angesehen, wenn sie aktuell noch nicht identifiziert ist, aber anhand von vorhandenen Informationen mit zumutbarem Aufwand direkt oder indirekt, bspw durch Zuordnung zu einer Kennung wie einem Namen oder anderen Merkmalen, die Ausdruck der physischen, wirtschaftlichen, kulturellen, etc Identität sind, identifiziert werden kann.[29]

Um in den Schutzbereich der DSGVO zu fallen, müssen personenbezogene Daten verarbeitet werden. Darunter fällt jeder Vorgang im Zusammenhang mit personenbezogenen Daten, wie etwa das Erheben, Erfassen, Ordnen, Speichern, Abfragen etc dieser Daten (Art 4 Z 2 DSGVO). Es kommt hierbei nicht darauf an, ob die Verarbeitung mit Hilfe automatisierter oder digitaler Verfahren stattfindet, weshalb bspw auch die Organisation von personenbezogenen Daten in Papierakten unter bestimmten Voraussetzungen eine Verarbeitung iSd DSGVO darstellen kann.[30]

Personell ist die DSGVO einerseits auf „Verantwortliche“ anwendbar, worunter jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle fällt, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art 4 Z 7 DSGVO). Die DSGVO knüpft an die Rolle als Verantwortlicher bestimmte Verpflichtungen. So hat der Verantwortliche unter gewissen Voraussetzungen vor einer bestimmten Datenverarbeitung eine Datenschutz-Folgenabschätzung durchzuführen und Betroffene können ihre Rechte ihm gegenüber geltend machen. Der Verantwortliche hat überdies durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Verarbeitung personenbezogener Daten rechtmäßig erfolgt. Gibt es mehrere Verantwortliche, so haben diese eine Vereinbarung über die Aufteilung der datenschutzrechtlichen Verpflichtungen (Art 26 DSGVO) abzuschließen. Erfolgt die Datenverarbeitung allerdings lediglich im Auftrag eines Verantwortlichen und legt man selbst nicht die Zwecke und Mittel der Verarbeitung fest, ist man Auftragsverarbeiter (Art 4 Z 8 DSGVO). Diese Abgrenzung in der Rollenverteilung ist deshalb von Bedeutung, um den richtigen Prüfmaßstab hinsichtlich der datenschutzrechtlichen Pflichten festzulegen.[31]

Da es sich bei Datenschutz um ein Grundrecht handelt, folgt die DSGVO dem Grundsatz, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, außer es liegt ein Erlaubnistatbestand vor. Die möglichen Rechtsgrundlagen einer Datenverarbeitung sind in Art 6 DSGVO taxativ (erschöpfend) aufgezählt und umfassen bspw die Einwilligung der betroffenen Person, den Schutz lebenswichtiger Interessen der betroffenen Person oder das berechtigte Interesse des für die Verarbeitung Verantwortlichen.

[28] *Scheichenbauer*, Datenschutz für Vereine² 11.
[29] Vgl Art 4 Z 1 DSGVO und *Scheichenbauer*, Datenschutz für Vereine² 11.
[30] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 13.
[31] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 25.

## Artikel 6 DSGVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Handelt es sich bei den verarbeiteten Daten um besondere Kategorien von personenbezogenen Daten iSd Art 9 DSGVO – sog „sensible Daten“ – so legt die DSGVO strengere Maßstäbe an.[32] Unter sensiblen Daten versteht man personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, einschließlich genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art 9 Abs 1 DSGVO). Die Verarbeitung dieser Kategorien von personenbezogenen Daten ist besonders heikel, da sie die intimsten Lebensbereiche betreffen und mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten von betroffenen Personen einhergehen können (ErwGr 51 DSGVO), weshalb deren Verarbeitung (zusätzlich zum Vorliegen einer Rechtsgrundlage

[32] Vgl *Scheichenbauer*, Datenschutz für Vereine² 33.

nach Art 6 Abs 1 DSGVO[33]) nur unter den strengen Voraussetzungen des Art 9 Abs 2 DSGVO zulässig ist (bspw mit der Einwilligung der betroffenen Person oder aus Gründen des öffentlichen Interesses).

Auf jeden Fall muss die Datenverarbeitung im Einklang mit bestimmten allgemeinen Grundsätzen erfolgen, die im gesamten Anwendungsbereich der DSGVO Relevanz entfalten.[34] Art 5 Abs 1 nennt bestimmte Verarbeitungsgrundsätze, die trotz ihrer Abstraktheit als Bestandteil der DSGVO unmittelbare Geltung als Pflichten entfalten und die Betroffenenrechte um eine objektive Dimension ergänzen.[35] Sie können als eine „Kurzdarstellung der DSGVO" in Gestalt verbindlicher Grundsätze verstanden werden, welche weitgehend in den Art 5 ff DSGVO konkretisiert werden.[36]

1. **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:** Die Verarbeitung muss in einer für die betroffene Person nachvollziehbaren Weise erfolgen und darf nur stattfinden, wenn sie von einem der zuvor beschriebenen Erlaubnistatbestände gedeckt ist. Insbesondere der Grundsatz der Transparenz ist für den gegenständlichen Bericht von Bedeutung, da darin bereits die Pflicht angelegt ist, keine heimlichen Datenverarbeitungen durchzuführen[37] sowie Informationen über die Datenverarbeitung in einfacher und klarer Sprache an betroffene Personen zu kommunizieren, worauf sich die Informationspflichten der Art 13 und 14 sowie das Auskunftsrecht nach Art 15 DSGVO in ihrem Kern gründen.[38] Die Einhaltung dieses Prinzips setzt voraus, dass Betroffene umfangreich darüber aufgeklärt werden, wozu ihre Daten verarbeitet werden und ordnungsgemäß sowie umfassend über die Bedingungen der Datenerhebung informiert werden.[39] Dies gilt sowohl für vergangene als auch zukünftige Datenverarbeitungen.[40]
2. **Zweckbindung:** Eine Datenverarbeitung darf nur für festgelegte, eindeutige und legitime Zwecke erfolgen und Daten dürfen nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Der Zweck muss dazu konkret und nicht in pauschaler Weise dokumentiert werden und rechtskonform sein.[41] Zwar kann der Zweck grundsätzlich vom Verantwortlichen selbst definiert werden, er ist allerdings intern zu dokumentieren (im Verarbeitungsverzeichnis) und extern (gegenüber der betroffenen Person) offenzulegen.[42] Der Grund dieser Zweckbindung liegt im Schutz der betroffenen Person durch die Begrenzung einer uneingeschränkten und unkontrollierten Datenverwendung.[43]
3. **Datenminimierung:** Die Datenverarbeitung muss für den Zweck erheblich sein und

[33] Vgl EuGH 21. 12. 2023, C-667/21, *Krankenversicherung Nordrhein,* ECLI:EU:C:2023:1022.
[34] Vgl *Köllmann*, Implementierung 198.
[35] Vgl *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kommentar[4] (2024) Art 5 DSGVO Rz 1.
[36] *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG[8] (2024) Art 5 DSGVO Rz 1.
[37] Vgl *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung[4] Art 5 DSGVO Rz 18.
[38] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 164.
[39] Vgl *Scheichenbauer*, Datenschutz für Vereine² 18.
[40] MwN *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer[8] Art 5 DSGVO Rz 17.
[41] Vgl *Köllmann*, Implementierung 203; *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 165.
[42] Vgl *Scheichenbauer*, Datenschutz für Vereine² 19.
[43] Vgl *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer[8] Art 5 DSGVO Rz 23.

auf das dafür notwendige Maß beschränkt sein. Dieser Grundsatz erlangt vor allem wegen der zunehmenden Bedeutung von Big-Data-Anwendungen besondere Relevanz, da es immer einfacher wird, riesige Datenmengen zu verarbeiten und somit eine rechtliche Begrenzung erforderlich ist.[44] Dem Grundsatz der Datenminimierung ist angemessen Rechnung getragen, wenn die Datenverarbeitung den festgelegten Zweck fördert und umgekehrt keine Daten verarbeitet werden, sofern der Verarbeitungszweck auch ohne sie erreicht werden kann.[45] Hier ist zu bedenken, ob der Zweck bspw auch mit aggregierten Daten (Wertintervalle anstelle genauer Werte) oder mit anonymisierten Daten erreicht werden kann.[46] Das Erfordernis der Angemessenheit der Datenverarbeitung bezieht sich darauf, ob der mit der Verarbeitung angestrebte Zweck überhaupt mit den angedachten personenbezogenen Daten erreicht werden kann und das Prinzip der Erheblichkeit fragt nach der Eignung bestimmter Datenarten für die verfolgten Zwecke.[47]

4. **Richtigkeit:** Daten haben sachlich richtig und - soweit erforderlich - auf dem neuesten Stand zu sein. Es gilt der Leitsatz, dass die verarbeiteten Daten zu jeder Zeit die Realität bestmöglich widerspiegeln müssen.[48] Es müssen Maßnahmen getroffen werden, um Daten, die diesem Erfordernis nicht entsprechen, zu löschen oder zu berichtigen. Dieser Grundsatz korrespondiert somit mit dem Recht auf Berichtigung nach Art 16 DSGVO und dem Recht auf Löschung gem Art 17 DSGVO.[49] Außerdem werden gewisse Aktualisierungspflichten insb bei einer langfristigen Aufbewahrung angenommen, wobei der Verantwortliche nicht in jedem Fall einen erheblichen Aufwand betreiben muss.[50]
5. **Speicherbegrenzung:** Daten, die eine Identifizierung einer betroffenen Person ermöglichen, dürfen nicht länger als für die Verarbeitungszwecke unbedingt erforderlich gespeichert werden. Personenbezogene Daten sollen damit zweckentsprechend nur eine begrenzte „Lebenszeit“[51] haben und entweder nach einer bestimmten Zeit gelöscht oder deren Personenbezug beseitigt werden.[52] Um das Prinzip der Speicherbegrenzung umzusetzen, sollte der Verantwortliche regelmäßig Überprüfungen der Daten und Fristen für die Löschung vorsehen und diese auch iSd Informationspflichten nach den Art 13 und 14 DSGVO kommunizieren.[53]
6. **Integrität und Vertraulichkeit:** Es muss eine angemessene Sicherheit für personenbezogene Daten bei der Verarbeitung sowie deren Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung gewährleistet werden. Im Ergebnis bedeutet dies die Pflicht, die personenbezogenen Daten vor Verfälschung („Integrität“) und vor Kenntnisnahme

[44] Vgl *Köllmann*, Implementierung 205.
[45] MwN *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung[4] Art 5 DSGVO Rz 57.
[46] Vgl *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung[4] Art 5 DSGVO Rz 57 f.
[47] MwN *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer[8] Art 5 DSGVO Rz 39 f.
[48] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung[2] 168.
[49] Vgl *Köllmann*, Implementierung 205.
[50] Vgl *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer[8] Art 5 DSGVO Rz 44 ff.
[51] Vgl *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer[8] Art 5 DSGVO Rz 50.
[52] Vgl *Scheichenbauer*, Datenschutz für Vereine[2] 20.
[53] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung[2] 169; *Köllmann*, Implementierung 206.

durch Unbefugte („Vertraulichkeit“) zu schützen.[54] Dieser Grundsatz wird in Art 32 DSGVO durch spezifische Vorgaben für eine sichere Datenverarbeitung konkretisiert.[55]

In Abs 2 normiert Art 5 überdies eine **Rechenschaftspflicht** des Verantwortlichen, der die Einhaltung dieser Verarbeitungsgrundsätze nachweisen können muss. Dies sorgt für einen beträchtlichen Mehraufwand bei der Erfüllung der damit verbundenen Dokumentationspflichten, da beispielsweise Einwilligungen nachweisbar sein müssen oder der Verantwortliche dokumentieren muss, dass er die Betroffenenrechte und Informationspflichten erfüllt hat.[56]

Dieser Auszug aus den wichtigsten Grundsätzen der DSGVO zeugt deutlich von dem Hauptanliegen dieses Regelwerks, nämlich der Stärkung von Betroffenenrechten, welche die DSGVO in Kapitel III (Art 12 bis 23) taxativ aufzählt.[57] Neben den antragsbedürftigen Betroffenenrechten, wie etwa dem Berichtigungs- oder Auskunftsanspruch, nehmen auch die Informationspflichten nach der DSGVO einen hohen Stellenwert ein. Denn nur wenn eine Person über die sie betreffenden Verarbeitungsvorgänge Bescheid weiß, ist sie in der Lage, ihre Rechte durchzusetzen, weshalb die Informationspflichten vom Verantwortlichen antragsunabhängig zu erfüllen sind.[58] Daher – wie auch ErwGr 39 DSGVO zu entnehmen ist – sollen Informationen an die betroffenen Personen die Transparenz der Verarbeitungsvorgänge erhöhen und die effektive Ausübung von Betroffenenrechten ermöglichen.[59] Die für den gegenständlichen Bericht relevanten Bestimmungen werden in Kapitel 5.4 im Detail vorgestellt.

[54] Vgl *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer[8] Art 5 DSGVO Rz 55.
[55] Vgl *Köllmann*, Implementierung 206.
[56] Vgl *Scheichenbauer*, Datenschutz für Vereine² 21.
[57] Vgl *Scheichenbauer*, Datenschutz für Vereine² 70.
[58] Vgl *Scheichenbauer*, Datenschutz für Vereine² 70.
[59] Vgl *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 240.

## 5.2.2 AI Act

### 5.2.2.1 Einleitung

Wie bereits in der Einleitung erwähnt, stellt die im Juli 2024 im Amtsblatt der EU publizierte KI-Verordnung (im Folgenden nach dem Englischen AI Act) den Endpunkt der Bemühungen der EU dar, eine erste europaweite horizontale, dh sektorunabhängige, Regulierung von KI zu schaffen. Dem AI Act gehen dabei zahlreiche immer konkreter werdende Aktivitäten auf EU-Ebene, die von Erklärungen, über ethische Leitlinien bis hin zum sog Weißbuch über KI reichen,[60] voran.

Es handelt sich beim AI Act in seiner ursprünglichen Konzeption vor allem um Produktsicherheitsrecht,[61] ähnlich bspw der Medizinprodukteverordnung.[62] Dieser Ansatz wurde später, vor allem aufgrund von Bemühungen des EP, um Betroffenenrechte wie dem Recht auf Erklärung „angereichert".

Der AI Act verfolgt dabei eine „multiple" Zielsetzung, bestehend einerseits aus der Verbesserung des Funktionierens des Binnenmarktes und der Förderung der "Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz". Andererseits soll dabei „gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte [...] vor schädlichen Auswirkungen von KI-Systemen in der Union" gewährleistet und Innovation unterstützt werden (Art 1 Abs 1 AI Act).

### 5.2.2.2 Anwendungsbereich

In Bezug auf den Anwendungsbereich des AI Act wird auf **sachlicher Ebene** primär auf den Begriff des KI-Systems (Art 3 Z 1 AI Act) abgestellt. Die Definition des KI-Systems war dabei einer der Hauptdiskussionspunkte im „Gesetzgebungsprozess".[63] Die finale Version definiert KI-Systeme anhand verschiedener Merkmale: maschinengestütztes System, unterschiedlicher Grad an Autonomie, mögliche Anpassungsfähigkeit nach Betriebsaufnahme,

[60] MwN *Hilgendorf*, Entstehungsgeschichte und Leitwerte, in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 1 (10 ff); *Zenner*, Entstehungsgeschichte, in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 1 (Rz 1 ff).

[61] Der AI Act folgt dabei dem sog New Legislative Framework (NLF), einem EU-Konzept der Produktregulierung mit gleichförmigen Kernelementen (Konformitätsbewertungsverfahren, häufig kontrollierte Selbstregulierung, essentielle Anforderungen werden festgelegt und durch Standards konkretisiert), mwN *Ebers*, Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RDi 2021, 588 (589); *Veale/Zuiderveen Borgesius*, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97 (102).

[62] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) 178/2002 und der Verordnung (EG) 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (MPVO), ABl L 2017/117, 1.

[63] MwN *Burtscher/Fellner/Raabe-Stuppnig*, Klassifizierung und Risikobewertung von KI-Systemen nach dem Entwurf für ein EU Gesetz über Künstliche Intelligenz, ZIIR 2023, 382 (382); *Fülöp*, AI Act. Das Ende europäischer Innovation oder Gefahr für den Datenschutz? Dako 2023, 82 (82); *Gless/Janal*, Anwendungsbereich und Adressaten, in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der Europäischen Union zur Künstlichen Intelligenz (2023) 15 (18 ff).

Eingaben, explizite oder implizite Ziele, Ableitung von Outputs, die physische oder virtuelle Umgebungen beeinflussen können.

## Definition KI

Der Ausdruck **„KI-System“** bezeichnet ein **maschinengestütztes** System, das für einen in **unterschiedlichem Grade autonomen Betrieb** ausgelegt ist und das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und das aus den erhaltenen **Eingaben** für **explizite oder implizite Ziele ableitet**, wie **Ausgaben** wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können (Vgl Art 3 Z 1 AI Act).

Das wichtigste Abgrenzungsmerkmal darunter ist die Fähigkeit zur „Ableitung“,[64] die sowohl von Machine-Learning- als auch von logik- und wissensgestützten Systemen erfüllt werden kann. Nach ErwGr 12 sollte sich die Definition des KI-Systems „nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen“ und dabei helfen, diese „von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen“ abzugrenzen. Die Europäische Kommission veröffentlichte am 6. Februar 2025 (unverbindliche) Leitlinien, um den Begriff KI-System zu präzisieren.[65] Diese stellen ua klar, dass einfache Machine-Learning-Ansätze wie lineare Modelle nicht als KI-Systeme zu qualifizieren sind.

Im Hinblick auf den **zeitlichen Anwendungsbereich** des AI Act ist darauf hinzuweisen, dass er für verbotene Praktiken seit dem 2. Februar 2025 und für Hochrisiko-KI-Systeme, mit Ausnahme von Systemen nach Art 6 Abs 1 iVm Anhang I AI Act (siehe unten), am 2. August 2026 gilt (Art 113 AI Act). Art 111 Abs 2 AI Act enthält dabei jedoch eine sog „grandfathering“-Klausel, nach der der AI Act für Betreiber von Hochrisiko-KI-Systemen, die vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden, nur dann gilt, wenn diese Systeme danach in ihrer Konzeption erheblich verändert wurden. Auf solche Hochrisiko-KI-Systeme würde somit auch das Recht auf Erklärung nach Art 86 AI Act keine Anwendung finden, da sie nicht dem AI Act unterliegen. Jedoch ist darauf hinzuweisen, dass in vielen Fällen eine Anpassung des Systems und damit eine erhebliche Veränderung notwendig sein wird, um Compliance mit anderen Rechtsvorschriften zu wahren (zB Antidiskriminierungsrecht, Schutzpflichten des Gesetzgebers, Datenschutzrecht). So wurde bspw in Bezug auf den „AMS-Algorithmus“ kritisiert, dass dieser, da er vor der COVID-19-Pandemie erstellt wurde, nicht die aktuelle Lage am Arbeitsmarkt widerspiegeln würde.[66] In einem solchen Fall müsste das System aktualisiert werden, was dazu führen würde, dass es in den Anwendungsbereich

[64] MwN *Wendehorst/Nessler/Aufreiter/Aichinger*, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605.
[65] Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final.
[66] *Wimmer*, AMS-Algorithmus. „Seit Corona ist Datenbasis wertlos“, https://futurezone.at/netzpolitik/ams-algorithmus-seit-corona-ist-datenbasis-wertlos/401101638 (Stand 18. 11. 2020).

des AI Act fallen würde. Ein „Missbrauch“ dieser Klausel durch (dauerhafte) „Verweigerung“ der Aktualisierung scheint somit nur begrenzt möglich.

In Bezug auf den **personellen Anwendungsbereich** ist innerhalb der relevanten Akteure primär zwischen Anbietern von KI-Systemen,[67] dh vorrangig Entwicklern, und Betreibern,[68] dh professionellen Nutzern, die das KI-System in eigener Verantwortung, also auf eigene Rechnung bzw auf eigenes Risiko, verwenden, zu unterscheiden. Der Großteil der Anforderungen richtet sich dabei an Anbieter von KI-Systemen.[69] Der Anwendungsbereich des AI Act betrifft dabei primär Anbieter, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind. Weiter erfasst sind auch Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder sich in der Union befinden. Mit dieser Formulierung sollen juristische Personen, Personengesellschaften ebenso wie natürliche Personen erfasst werden, dh am Sitz oder gewöhnlichen Aufenthalt angeknüpft werden.[70] Subsidiär fallen auch Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, in den Anwendungsbereich, wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird.

Der AI Act folgt einem risikobasierten Ansatz.[71] Dieser soll die Verhältnismäßigkeit der Maßnahmen garantieren: Je höher das Risiko, primär gemessen anhand der Betroffenheit von Grundrechten, desto umfangreicher die Regulierung. Durch diese Proportionalität soll sichergestellt werden, dass Innovation nicht unnötig gehemmt wird. Für dieses Projekt von Relevanz ist dabei primär die Gruppe der Hochrisiko-KI-Systeme, auf die Art 86 AI Act anwendbar ist. Darüber hinaus verbietet der AI Act auch gewisse Praktiken, da diese den grundlegenden Werten der Union entgegenstehen. Diese gilt es von den relevanten Hochrisiko-KI-Systemen abzugrenzen, da sie sich in manchen Bereichen oder in Bezug auf manche KI-Systeme überschneiden können.

Daneben bestehen insbesondere Transparenzpflichten für bestimmte Systeme mit – im Verhältnis zu den zuvor genannten Stufen – niedrigerem Risikopotenzial.[72] Dabei ist anzumerken, dass die Transparenzpflichten auch (eingeschränkt) für Hochrisiko-KI-Systeme gelten können und somit keine eigenständige, losgelöste Stufe darstellen. Unabhängig von der Einordnung des KI-Systems gelten zudem die Anforderungen an die notwendige KI-Kompetenz gem Art 4 AI Act. Auch die Regelungen über KI-Reallabore (Art 57 ff AI Act) zielen prinzipiell nicht explizit auf eine bestimmte Risikostufe ab.

---

[67] Dh “eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich“ (Art 3 Z 3 AI Act).

[68] Dh “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“ (Art 3 Z 4 AI Act).

[69] Zu beachten ist, dass es als Betreiber nach Art 25 AI Act unter gewissen Umständen, bspw bei Veränderung der Zweckbestimmung, möglich ist, zum (neuen) Anbieter zu werden.

[70] *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 2 Rz 21.

[71] MwN *Kaminski*, Regulating the Risks of AI, Boston University Law Review 2023, 1347.

[72] Vgl ErwGr 26 AI Act.

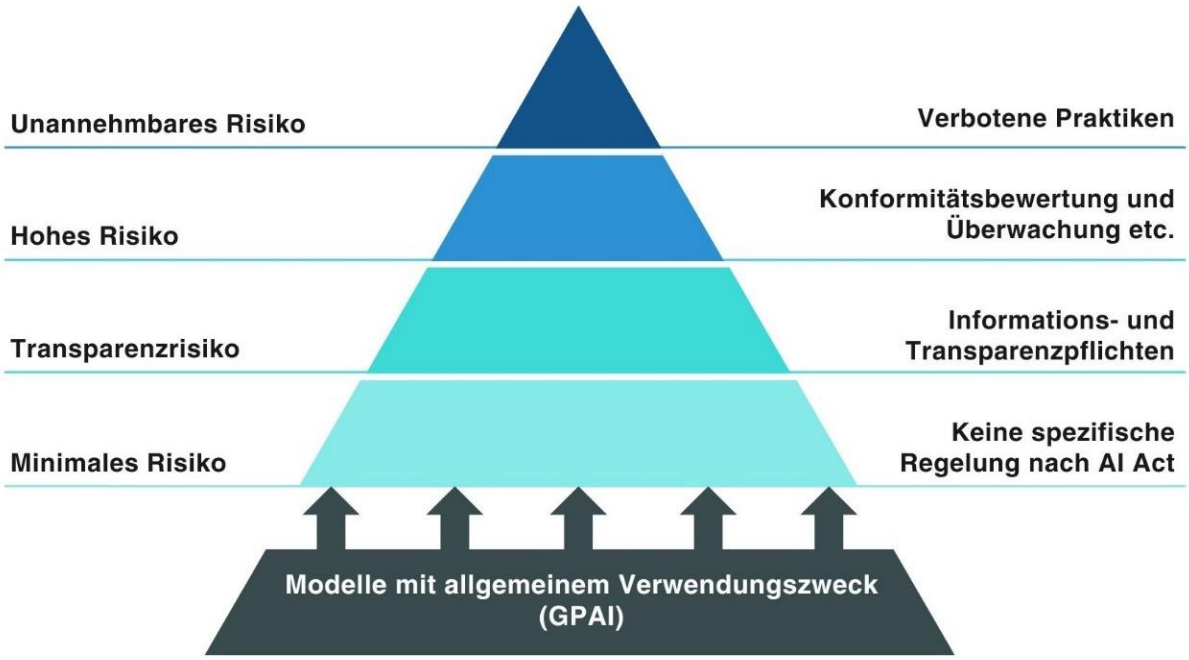


Abbildung 2: Eigene Darstellung der Risikostufen des AI Act in Anlehnung an die Pyramide der EU Kommission[73]

#### 5.2.2.3 Verbotene Praktiken

Wie ErwGr 28 ausführt, kann KI „auch missbraucht werden und neue und wirkungsvolle Instrumente für manipulative, ausbeuterische und soziale Kontrollpraktiken bieten." Da diese Praktiken „besonders schädlich und missbräuchlich" sind, sollten sie „verboten werden, weil sie im Widerspruch zu den Werten der Union stehen". Es geht demnach um KI-Praktiken, die ein inakzeptables Risiko bergen.[74] Diese verbotenen Praktiken werden in Art 5 AI Act gelistet.[75]

Die folgenden verbotenen Praktiken sind für das Projekt von besonderer Bedeutung, da sie ähnliche Bereiche wie manche der Use Cases betreffen und daher entsprechend unterschieden werden müssen:

- KI-Systeme, die Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzen, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte

[73] Vorlage: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf
[74] Vgl insbesondere ErwGr 26 und 179 AI Act; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final), 5.2.2.
[75] MwN *Neuwirth*, Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA), CLSR 2023, 1 (3 ff); *Rostalski/Weiss*, Verbotene KI-Praktiken, in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der Europäischen Union zur Künstlichen Intelligenz (2023) 35.

Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird. (Art 5 Abs 1 lit a AI Act)

- KI-Systeme, die eine Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung ausnutzen, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird. (Art 5 Abs 1 lit b AI Act)
- KI-Systeme zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen. (Art 5 Abs 1 lit f AI Act)

Dabei stellt sich die Frage, ob bspw die Schaltung von Werbung (zB bei spielsüchtigen Personen) ihre Vulnerabilität ausnutzt und damit unter das Verbot fallen würde. Komplexe Abgrenzungsprobleme ergeben sich auch in Bezug auf Emotionserkennung, die am Arbeitsplatz und in Bildungseinrichtungen verboten ist, aber außerhalb dieser Bereiche unter die Gruppe der Hochrisiko-KI-Systeme fällt (Näheres dazu findet sich in Abschnitt 5.3.4).

#### 5.2.2.4 Hochrisiko-KI-Systeme

Im Rahmen der Risiko-Stufen des AI Act stellen „Hochrisiko-KI-Systeme“ die nächste Stufe nach verbotenen KI-Praktiken dar und dabei auch jenen Bereich, für den die Verordnung die meisten Regelungen bereithält (Art 6 bis 49 AI Act).

Der AI Act sieht dabei zwei Wege zur Klassifizierung als Hochrisiko-KI-System vor:

- Erstens „eingebettete Hochrisiko-KI-Systeme“, dh Produkt- oder Sicherheitskomponenten gem Art 6 Abs 1 AI Act, die bereits in den Geltungsbereich des EU-Produktsicherheitsrechts fallen (bspw Medizinprodukte).[76] Diese Kategorie spielt für das gegenständliche Projekt keine Rolle.
- Zweitens „eigenständige Hochrisiko-KI-Systeme“ gem Art 6 Abs 2 AI Act, die in Anhang III, der acht risikoreiche Anwendungsbereiche und konkrete Anwendungsfälle beschreibt, definiert werden.

Im Anhang (siehe Abschnitt 9.1) findet sich eine Liste mit einem Überblick über die jeweiligen Hochrisiko-KI-Bereiche in Anhang III AI Act mit entsprechenden Spezifikationen.

Auch wenn das KI-System in einem der in Anhang III AI Act aufgelisteten Bereiche eingesetzt

[76] MwN *Martini*, Hochrisiko-KI-Systeme. Risikobasierter Ansatz, in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 51 (62 ff); *Schwartmann/Pottkämper*, Hochrisiko-KI-Systeme gem Art. 6 Abs. 1 KI-VO (Anhang I), in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 152 (Rz 152 ff).

wird, kann eine Ausnahme von der Einstufung als Hochrisiko-KI-System vorliegen, „wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst“ (Art 6 Abs 3 AI Act).

Diesbezüglich werden vier alternative Bedingungen genannt:

- das KI-System ist dazu bestimmt, eine eng gefasste Verfahrensaufgabe durchzuführen (bspw Umwandlung von unstrukturierten Daten in strukturierte Daten, Einordnung von eingehenden Dokumenten in Kategorien, Erkennung von Duplikaten)
- das KI-System ist dazu bestimmt, das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern (bspw Verbesserung der Sprache von bereits erfassten Dokumenten, zB professioneller Ton oder wissenschaftlicherer Sprachstil)
- das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu gedacht, die zuvor abgeschlossene menschliche Bewertung ohne eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen (bspw um in Bezug auf Benotungsmustern eines Lehrers nachträglich zu prüfen, ob der Lehrer möglicherweise von dem Benotungsmuster abgewichen ist, um so auf mögliche Unstimmigkeiten oder Unregelmäßigkeiten aufmerksam zu machen)
- das KI-System ist dazu bestimmt, eine vorbereitende Aufgabe für eine Bewertung durchzuführen (bspw intelligente Lösungen für die Bearbeitung von Dossiers, zB verschiedene Funktionen wie Indexierung, Suche, Text- und Sprachverarbeitung oder Verknüpfung von Daten mit anderen Datenquellen; KI-Systeme, die für die Übersetzung von Erstdokumenten verwendet werden)

Anbieter, die der Ansicht sind, dass in Anhang III angeführte KI-Systeme nicht hochriskant wären, müssen die entsprechende Bewertung vor dem Inverkehrbringen oder der Inbetriebnahme des Systems dokumentieren, wobei sie diese Dokumentation auf Verlangen den zuständigen nationalen Behörden vorzulegen haben, und unterliegen der Registrierungspflicht gemäß Art 49 Abs 2 AI Act (Art 6 Abs 4 AI Act).

Aufgrund der Auswahl der Use Cases sind für dieses Projekt folgende Bereiche in Anhang III von Relevanz:

- Z 1 „Biometrie“, der „KI-Systeme, die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen“ (lit c) beinhaltet.
- Z 5 „Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen“, der „KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen“ (lit b) und „KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen“ (lit c) umfasst.

Im Folgenden werden die Anwendungsbereiche, die sich aus Z 1 sowie Z 5 ergeben, in groben Zügen erläutert.

### Emotionserkennungssysteme

*Emotionserkennungssystem* bezeichnet „ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten“ (Art 3 Z 39 AI Act). Biometrische Daten sind dabei „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische Daten“ (Art 3 Z 34 AI Act).[77] Dabei können Daten über den Gang, die Stimme, die Tastenanschläge, die Blickrichtung, die Gestik, Herzfrequenz, Körpertemperatur, Hautleitfähigkeit verarbeitet werden.[78]

Emotionserkennung gem AI Act umfasst die Erkennung und Ableitung verschiedener Emotionen mit Ausnahme physischer Zustände (Schmerz, Müdigkeit). Einfache, offensichtliche Emotionen (Lachen, einfache Gesten, Sprechlautstärke) sind ebenfalls nicht eingeschlossen (Siehe im Detail Abschnitt 5.3.4.).[79]

Anhang III Z 1 lit c zur Emotionserkennung ergänzt das Verbot „von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen“[80] (Art 5 Abs 1 lit f AI Act). Dieses könnte im gegenständlichen Projekt bei Verwendung von Emotionserkennungssystemen insbesondere am Arbeitsplatz von Bedeutung sein und würde zu einem Verbot solcher Systeme führen.

### Kreditwürdigkeitsprüfung und Bonitätsbewertung

Die Bewertung der Kreditwürdigkeit kann dabei, da von dieser Bewertung der Zugang zu Wohnraum, Strom und Telekommunikation abhängen kann, gravierende Auswirkungen auf die finanzielle Lebensgrundlage haben und gilt daher ebenfalls als hochriskant. Auch Systeme, die einen Kreditscore errechnen, bspw durch die SCHUFA, fallen unter diese Vorschrift.[81]

---

[77] Nach *Schwartmann/Keber/Steinbrück*, Emotionserkennungssysteme, in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 89 (Rz 90) bzw *Hansen/Nägele/Steinbrück*, Biometrische Identifizierung, Kategorisierung und Emotionserkennung natürlicher Personen, in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 165 (Rz 165) ist prinzipiell die datenschutzrechtliche Definition der biometrischen Daten (Art 4 Z 14 DSGVO) anwendbar, jedoch ohne Einschränkung in Bezug auf die eindeutige Identifizierung; siehe im Detail Abschnitt 5.3.4.

[78] *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 89 (Rz 90 f).

[79] MwN *Hansen/Nägele/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 165 (Rz 171).

[80] Eine Ausnahme besteht, wenn die Verwendung des KI-Systems aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden soll.

[81] *Schwartmann/Köhler*, Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen, in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 222 (Rz 224).

**Risikobewertung und Preisbildung im Fall von Lebens- und Krankenversicherungen**

Die Risikobewertung und Preisbildung im Fall von Lebens- und Krankenversicherungen wurde auf Bestreben des Europäischen Parlaments[82] aufgenommen und dient insbesondere der diskriminierungsfreien Sicherung des Lebensstandards.[83] Die Aufnahme als Hochrisiko-KI-System dient insofern neben der Wahrung der Gleichbehandlung auch dem Schutz vor opaken Entscheidungsstrukturen und damit einhergehenden erschwerten Rechtsschutzmöglichkeiten.[84]

Die Einstufung als „hochriskant" führt insofern zu einer besseren Eindämmung der Risiken, insbesondere durch Anforderungen an die Datenqualität (Art 10 AI Act), die Auswirkungen auf algorithmische Diskriminierung haben kann, die Notwendigkeit, ein Risikomanagementsystem einzurichten (Art 9 AI Act), Anforderungen an die Transparenz des Systems (Art 13 AI Act) und Anforderungen an die menschliche Aufsicht (Art 14 AI Act). Auf Ebene der Betreiber führt diese Qualifikation auch zu verstärktem Schutz durch Aktivierung des Rechtes auf Erläuterung und potenziell der Grundrechts-Folgenabschätzung (Art 27 AI Act).

#### 5.2.2.5 Anforderungen an Hochrisiko-KI-Systeme

Art 8 bis 15 AI Act enthalten die zentralen Anforderungen an Hochrisiko-KI-Systeme. Diese sind primär an die Anbieter solcher Systeme gerichtet und werden in einem sog Konformitätsbewertungsverfahren überprüft. Im Hinblick auf das Projektziel werden im Folgenden nur Anforderungen erläutert, die einen Konnex zu Art 86 AI Act und zum Themenfeld Transparenz aufweisen. Die Ausführungen sind dabei knappgehalten, da Anbieterpflichten nicht im Zentrum des Projektes stehen, weil sich Art 86 AI Act an Betreiber richtet.

**Technische Dokumentation (Art 11 AI Act)**

Art 11 AI Act normiert, dass bevor ein Hochrisiko-KI-System in Verkehr gebracht oder in Betrieb genommen wird, eine technische Dokumentation zu erstellen und auf dem neuesten Stand zu halten ist. Die technische Dokumentation dient primär im Konformitätsbewertungsverfahren als Nachweis, dass das KI-System die Anforderungen der Art 8-15 AI Act erfüllt. Sie richtet sich somit primär an notifizierte Stellen, die die Konformität bewerten, und (nationale) Behörden. Ihre Mindestinhalte werden in Anhang IV konkretisiert.[85]

---

[82] Siehe zu diesem Punkt bereits die Forderung nach der Definition als Hochrisiko-KI-System in *Wendehorst*, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021), https://www.sozialministerium.at/dam/sozialministeriumat/Anlagen/Themen/Konsumentenschutz/Konsumentenpolitik/The-Proposal-for-an-Artificial-Intelligence-Act-COM2021-206-from-a-Consumer-Policy-Perspective_dec2021__pdfUA.pdf .

[83] *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner* Rz 222 (Rz 229).

[84] *Ruschemeier* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Anhang III Rz 48.

[85] MwN *Spindler*, Anforderungen an Hochrisiko-KI-Systeme (außer Transparenz), in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 93 (104 f).

Die technische Dokumentation könnte auch für Betreiber von Bedeutung sein, bspw um eine eigene Risikoeinschätzung vornehmen zu können.[86]

### Aufzeichnungspflichten (Art 12 AI Act)

Art 12 AI Act normiert im Sinne der Rückverfolgbarkeit,[87] dass die Technik der Hochrisiko-KI-Systeme die automatische Aufzeichnung von Ereignissen, dh Protokollierung, ermöglichen muss. Damit wird auch die Black-Box-Problematik adressiert.[88]

Diese Funktion muss die Aufzeichnung von Ereignissen ermöglichen, die für die Ermittlung von Situationen, die dazu führen können, dass das Hochrisiko-KI-System ein Risiko birgt oder dass es zu einer wesentlichen Änderung kommt, die Erleichterung der Beobachtung nach dem Inverkehrbringen und die Überwachung des Betriebs der Hochrisiko-KI-Systeme relevant sind.

### Transparenz und Bereitstellung von Informationen für die Betreiber (Art 13 AI Act)

Der stärkste Konnex zwischen Art 86 AI Act und den Anforderungen an Hochrisiko-KI-Systeme besteht mit Art 13 AI Act. Dieser normiert Transparenzverpflichtungen für Anbieter von Hochrisiko-KI-Systemen gegenüber Betreibern und besteht aus zwei Komponenten. Einerseits bestimmt Art 13 Abs 1 AI Act, dass Hochrisiko-KI-Systeme „so konzipiert und entwickelt [werden], dass ihr Betrieb hinreichend transparent ist, damit die Betreiber die Ausgaben eines Systems angemessen interpretieren und verwenden können." Es handelt sich um eine funktionelle Form von Transparenz, die auf die Nutzbarkeit des Systems und zur Einhaltung der (anderen) Anforderungen des AI Act beitragen soll.[89] Wie in der Literatur angemerkt, wird, da die Vorschrift keine konkreten Maßnahmen beinhaltet, die (konkrete) Umsetzung den Anbietern überlassen.[90] Dies führt zu einem Maß an Rechtsunsicherheit. So wird bspw auf Konkretisierung durch (kommende) technische Standards, Leitfäden und Rechtsprechung verwiesen.[91]

Andererseits normiert Art 13 Abs 2 AI Act, dass Hochrisiko-KI-Systeme „mit Betriebsanleitungen in einem geeigneten digitalen Format bereitgestellt oder auf andere Weise mit Betriebsanleitungen versehen [werden], die präzise, vollständige, korrekte und eindeutige Informationen in einer für die Betreiber relevanten, barrierefrei zugänglichen und verständlichen Form enthalten".

Art 13 Abs 3 AI Act listet die Mindestelemente dieser Anleitung bspw die Merkmale, Fähigkeiten und Leistungsgrenzen des Hochrisiko-KI-Systems, die Maßnahmen zur

[86] *Hansen*, Technische Dokumentation (Art. 11 KI-VO) in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 309 (Rz 312).
[87] *Schwartmann/Keber/Köhler*, Aufzeichnungspflichten (Art. 12), in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 319 (Rz 319 f).
[88] *Kumkar*, Transparenzanforderungen an Hochrisiko- und andere KI-Systeme, in *Hilgendorf/Roth-Isigkeit* (Hrsg), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 109 (112).
[89] *Kumkar* in *Hilgendorf/Roth-Isigkeit* 109 (113).
[90] MwN *Schneeberger*, Machine Learning in der Verwaltung. Rechtsfragen der Black-Box-Problematik (2024) 424.
[91] *Schwartmann/Keber/Köhler*, Transparenz und Bereitstellung von Informationen für die Betreiber (Art. 13), in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 329 (Rz 332).

Gewährleistung der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Betreibern die Interpretation der Ausgaben von Hochrisiko-KI-Systemen zu erleichtern und gegebenenfalls eine Beschreibung der in das Hochrisiko-KI-System integrierten Mechanismen, die es den Betreibern ermöglicht, die Protokolle ordnungsgemäß zu erfassen, zu speichern und auszuwerten.[92]

Diese Informationen aus der Betriebsanleitung dürften logistisch eine wichtige Quelle für das Recht auf Erklärung gem Art 86 AI Act sein.

[92] *Schwartmann/Keber/Köhler* in *Schwartmann/Keber/Zenner* Rz 329 (Rz 335 ff).

## 5.3 Praxisbeispiele und rechtliche Einordnung in den Anwendungsbereich

Da das Recht oftmals abstrakt ist und daher die Umlegung der rechtlichen Analyse auf die Praxis eine Herausforderung darstellen kann, arbeitet der gegenständliche Bericht mit Fallbeispielen, um die rechtliche Relevanz der behandelten Vorgaben praktisch greifbar zu machen. Bei der Auswahl der Praxisbeispiele wurde darauf geachtet, für Unternehmen und Konsument:innen relevante Anwendungsbereiche der rechtlichen Bestimmungen zu illustrieren, um damit einen praktischen Mehrwert zu schaffen.

Dazu erfolgt zunächst eine detaillierte Sachverhaltsdarstellung der ausgewählten Use Cases, wobei schon eine erste rechtliche Einordnung in den Anwendungsbereich der DSGVO und des AI Act vorgenommen wird. Diese Ausführungen bilden die Grundlage für die weitere rechtliche Analyse von Art 86 AI Act, die anhand der Fallbeispiele vorgenommen wird. Der einschlägige Abschnitt 5.5. nimmt daher immer wieder auf die Use Cases Bezug und beinhaltet neben einer theoretischen Abhandlung auch eine schrittweise Prüfung, ob die Use Cases in den Anwendungsbereich von Art 86 AI Act fallen und wie sich dessen Vorgaben praktisch veranschaulichen lassen. Die wichtigsten Erkenntnisse der Analyse von Art 86 AI Act sowie die Lösung der Fallbeispiele werden anschließend in Abschnitt 5.7. zusammengefasst und im Hinblick auf die einzelnen Use Cases in einer Tabelle vergleichend dargestellt.

### 5.3.1 Preisbildung Lebens- und Krankenversicherung (Use Case 1)

#### 5.3.1.1 Allgemeines

Personalisierte bzw dynamische Preisgestaltung hält zunehmend in vielen Bereichen der Privatwirtschaft wie der Hotelindustrie,[93] bei Flügen oder in Online-Shops Einzug.[94] Auch Versicherungsunternehmen bedienen sich Ansätzen wie Profiling für die Risikoabschätzung bei der Vergabe von Polizzen (zB bei Kfz-Haftpflichtversicherungen auf der Grundlage des Fahrstil-Risikoprofils oder bei Krankenversicherungen unter Berücksichtigung möglicher Gesundheitsrisikofaktoren).[95]

So ist beispielsweise denkbar, dass eine Kranken- oder Lebensversicherung Daten über das Einkaufsverhalten ihrer Versicherungsnehmer:innen erhält und diese nutzt, um durch Profiling-Analysen „kostenintensive“ Versicherungsnehmer:innen zu identifizieren (zB Identifizierung von Versicherungsnehmer:innen, die mit einer hohen Wahrscheinlichkeit an einer schwerwiegenden Krankheit leiden werden).[96]

[93] *red*, Mehr Umsatz. Forscher rät Hoteliers zu KI, https://salzburg.orf.at/stories/3269685/ (Stand 20. 8. 2024).
[94] MwN *Hafner-Thomic*, Personalisierte Preise im Online-Handel. Eine Untersuchung aus datenschutz-, verbraucher- und wettbewerbsrechtlicher Sicht (2024) 1 ff.
[95] *Hafner-Thomic*, Preise 33.
[96] *Lorentz*, Profiling. Persönlichkeitsschutz durch Datenschutz? Eine Standortbestimmung nach Inkrafttreten der DSGVO (2020) 150.

Zu diesen Zwecken werden häufig auch Daten aus sozialen Netzwerken verarbeitet. So sollen Lebensversicherer versucht haben, die Lebenserwartung ihrer Kund:innen über deren Aktivitäten in sozialen Netzwerken zu berechnen. Dabei können Informationen aus diesen Netzwerken Aussagen darüber erlauben, ob eine Person einen aktiven Lebensstil führt oder viele Interessen hat, was für eine bessere Gesundheit spricht, oder ob die Person primär Zuhause bleibt. Darüber hinaus kann Profiling im Versicherungsbereich dafür eingesetzt werden, jene Kund:innen zu identifizieren, die kontinuierlich hohe Schäden verursachen.[97]

Gerade im Versicherungsbereich gibt es Bedenken, dass das tradierte Solidaritätsprinzip der gesetzlichen Versicherungen durch personalisierte Preisgestaltung aufgeweicht werden könnte, wenn nicht mehr alle Mitglieder den gleichen Beitrag zahlen, um die individuell unbekannten Gesundheitsrisiken aller Beitragszahlenden abzudecken.[98] Dabei ergeben sich auch Überschneidungen zu antidiskriminierungsrechtlichen Fragestellungen.[99]

#### 5.3.1.2 Rechtliche Beurteilung

Für die Zwecke der Preisbildung bei Lebens- und Krankenversicherungen werden häufig Persönlichkeitsprofile herangezogen.[100] Es handelt sich dabei also um eine Form von Profiling, häufig im Kontext einer automatisierten Entscheidungsfindung iSv Art 22 DSGVO.

Der AI Act ordnet diesen Bereich den Hochrisiko-KI-Systemen zu. Er fällt unter die Gruppe der „Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen“ (Anhang III Z 5 lit c AI Act), „KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen“. ErwGr 58 AI Act begründet diese Einstufung damit, dass „KI-Systeme, die für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Kranken- und Lebensversicherungen eingesetzt werden, auch erhebliche Auswirkungen auf die Existenzgrundlage der Menschen haben und bei nicht ordnungsgemäßer Konzeption, Entwicklung und Verwendung schwerwiegende Konsequenzen für das Leben und die Gesundheit von Menschen nach sich ziehen [können], einschließlich finanzieller Ausgrenzung und Diskriminierung.“

### 5.3.2 Churn Predictions (Use Case 2)

Eines der Hauptziele der Vorhersage der Kundenabwanderung ist die Unterstützung bei der

[97] *Lorentz*, Profiling 22.
[98] *Hidar*, Rechtliche Grenzen smarter Preisgestaltung. Eine Untersuchung der rechtlichen Zulässigkeit dynamischer und personalisierter Preisgestaltung aus datenschutz- und lauterkeitsrechtlicher Perspektive (2021) 350.
[99] MwN *Bekkum/Zuiderveen Borgesius/Heskes*, AI, insurance, discrimination and unfair differentiation. An overview and research agenda[4], https://arxiv.org/abs/2401.11892 (Stand 31. 1. 2025); *Zuiderveen Borgesius*, Price Discrimination, Algorithmic Decision-Making, and European Non-Discrimination Law, European Business Law Review 2020, 401; *Zuiderveen Borgesius/Bekkum/Ooijen/Schaap/Harbers/Timan*, Discrimination and AI in insurance. What do people find fair? Results from a survey, https://arxiv.org/abs/2501.12897 (Stand 22. 1. 2025).
[100] *Lorentz*, Profiling 150.

Entwicklung von Möglichkeiten zur Kundenbindung. Modelle zur Vorhersage der Kundenabwanderung zielen darauf ab, frühe Abwanderungssignale zu erkennen und versuchen, die Kund:innen vorherzusagen, die das Unternehmen verlassen könnten. Die Abwanderungsvorhersage ist ein nützliches und zielführendes Instrument, um abwanderungsgefährdete Kund:innen zu identifizieren und sie durch geeignete Maßnahmen vom Bleiben zu überzeugen. In der Fachsprache wird die Vorhersage der Abwanderung von Kund:innen „Churn Prediction“ genannt.[101]

Regelmäßig liegt der Zweck der Verarbeitung in der Kundenbindung somit darin, durch zielgruppenorientierte Werbemaßnahmen die Kündigung von Verträgen durch das Anbieten von bestimmten Vorteilen an ausgewählte (aufrechte) Kundenbeziehungen zu vermeiden. Um die Auswahl solcher Kund:innen zu ermöglichen, werden regelmäßig aus bestehenden Datenbeständen an aufrechten Kundenbeziehungen aggregierte Daten erstellt, um daraus Aussagen, Wahrscheinlichkeiten und Interpretationen zum Kundenverhalten abzuleiten, um der Beendigung von Verträgen rechtzeitig durch Marketingmaßnahmen entgegenwirken zu können.

Die Verarbeitung („Stornoprävention“) gliedert sich dabei oftmals in mehrere, jeweils aufeinander aufbauende Abschnitte. In einem ersten Schritt können die aus dem internen Data Warehouse stammenden Kundendaten aggregiert aufbereitet werden (A.), in einem zweiten Schritt wird daraus pro aktivem Kundendatensatz ein Scorewert errechnet (B.). Schlussendlich werden mittels der Software Kundengruppe(n) analysiert und eine Zielgruppendefinition festgelegt. Die eigentliche Selektion der Personen kann im operativen Kampagnen-Management-System analog der vorangegangenen Zielgruppendefinition getroffen werden, die je nach Kundenbindungskampagne, mit Angeboten kontaktiert werden (C.). Im letzten Schritt erfolgt die Aussendung der Angebote an die ausgewählten Kund:innen (D.).

Betrachtet man die Verarbeitung schematisch, ergibt sich oftmals folgendes Bild: Die Daten der betroffenen Personen (Kund:innen) werden bei der Verarbeitung in vier Schritten verwendet: In einem ersten Schritt werden die Daten zu Analysezwecken, teilweise nur in aggregierter Form und teilweise in pseudonymisierter Form verarbeitet, im zweiten Schritt erfolgt eine Modellbildung (Gruppenbildung) mit Scorewerten als Ergebnis. Im dritten Schritt erfolgt die Zuordnung der Betroffenen zu den analysierten Zielgruppen und die Auswahl der konkreten Zielgruppe für die zielgruppenorientierten Werbemaßnahmen. Im letzten (vierten) Schritt findet die konkrete Bewerbung der identifizierten Kund:innen statt.

#### 5.3.2.1 Beispielhafter Ablauf Scoring

Mittels statistischer Methoden werden in diesem Schritt jene Kund:innen gefunden, bei denen die Storno-Wahrscheinlichkeit besonders hoch ist. Mittels eines künstlichen neuronalen Netzwerks werden die Quelldaten („Ausprägungen“) zu einem Modell geformt. Das entwickelte

[101] *Mittelstand-Digital Zentrum Spreeland*, Churn Prediction - Vorhersage von Kundenabwanderung mittels KI, https://www.digitalzentrum-spreeland.de/Kuenstliche-Intelligenz/KI-Blog/Churn-Prediction-Vorhersage-von-Kundenabwanderung-mittels-KI.html (abgerufen am 14. 2 . 2025).

Modell wird für jeden in Frage kommenden Bezug angewandt. Jeder Bezug erhält einen individuellen „Storno Score“.

Für das Stornoscoring-Modell werden signifikante Muster der Stornierenden jenen der Nicht-Stornierenden gegenübergestellt. Anschließend werden die Bezüge in mehrere Gruppen nach ihrer Storno-Wahrscheinlichkeit eingeteilt.

#### 5.3.2.2 Beispielhafter Ablauf Anwendung

Die Marketingabteilung wählt eine den Anforderungen entsprechend selektierte Personengruppe für die Kundenbindungskampagne aus. Derartige Marketingaktionen können zB „Gratismonate bei Verlängerung“, oder ähnliches sein. Im Kampagnenfokus steht dabei nicht die einzelne Person, sondern Personengruppen mit einem bestimmten Scorewert, welche nicht automatisch „vom System“ ausgewählt werden: Vielmehr liegt immer eine Intervention eines Menschen vor, die auf eine Geschäftsentscheidung zurückführbar ist und vom jeweiligen Abteilungsleiter bzw von der jeweiligen Abteilungsleiterin des Marketings festgelegt wird.

#### 5.3.2.3 Rechtliche Beurteilung

Verarbeitungstätigkeiten zu Kundenbindungszwecken können sich (je nach Beurteilung des Vertragszwecks) - auf Grundlage der bislang dazu erschienen Literatur - auf Art 6 Abs 1 lit b DSGVO (Vertragserfüllung) oder auf Art 6 Abs 1 lit f DSGVO (Interessenabwägung) stützen; eine einwilligungsbasierte Verarbeitung ist de facto in der Regel nicht möglich. Da hinsichtlich der Vertragserfüllung nicht geklärt ist, inwieweit die Zweckerfüllung bei Kundenbindungsprogrammen reicht, und in der Literatur überwiegend eine Interessenabwägung herangezogen wird, stützt sich die vorliegende Verarbeitung auf den Zulässigkeitsgrund des Art 6 Abs 1 lit f DSGVO.[102]

Nach *Gierschmann* sollte es möglich sein, dass man zumindest für einen normalen kaufmännischen Vertrieb übliche Verarbeitungen (zB Speicherung in einem CRM-System, Analyse des Kaufverhaltens zur Clusterung in A-B-C-Kund:innen, Analyse vorhandener Verträge, um Neuangebote zu prüfen) als noch vom ursprünglichen Zweck erfasst ansieht.[103]

Sofern eine kompatible Weiterverarbeitung iSd Art 6 Abs 4 DSGVO vorliegt, ist Art 13 Abs 3 DSGVO zu beachten, wonach der Verantwortliche den betroffenen Personen vor einer Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Art 13 Abs 2 zur Verfügung zu stellen hat.

Für den vorliegenden Anwendungsfall Stornoprävention/Churn Prediction ist festzuhalten,

[102] (Deutsche) *Datenschutzkonferenz*, Kurzpapier Nr. 3. Verarbeitung personenbezogener Daten für Werbung 1, https://www.lda.bayern.de/media/dsk_kpnr_3_werbung.pdf (Stand 29. 6. 2017).
[103] *Gierschmann*, Gestaltungsmöglichkeiten bei Verwendung von personenbezogenen Daten in der Werbung, MMR 2018, 7 (12).

dass es in der Regel zu keiner (voll-)automatisierten Entscheidungsfindung im Einzelfall nach Art 22 DSGVO kommt, da Verantwortliche mittels ihrer zuständigen Dienstnehmer:innen Kundengruppen auswählen, welchen idR spezifische Angebote gemacht werden.

Bei einem besonders eingreifenden Charakter des Profiling-Prozesses, wenn Personen webseiten-, geräte- oder diensteübergreifend verfolgt werden und etwa Personenkreise mit finanziellen Schwierigkeiten, die gezielt und regelmäßig Werbung für bestimmte Leistungen erhalten, kann die Lage anders zu beurteilen sein.

Grundsätzlich scheint es sich bei KI-Anwendungen aus dem Bereich der Churn Prediction/Stornoprävention zwar um Profiling, jedoch weder um verbotene Praktiken noch (mangels Aufzählung in Anhang III) um Hochrisiko-KI-Systeme im Sinne des AI Act zu handeln.

Hier ist jedoch zu beachten, dass diese Einstufung - je nach konkreter Ausgestaltung - auch anders ausfallen kann. So wäre etwa eine Kombination mit einem Emotionserkennungssystem denkbar und es könnte dann in weiterer Folge ein Hochrisiko-KI-System im Sinne des AI Act vorliegen.

### 5.3.3 Bonitätsprüfungen (Use Case 3)

Bonitätsprüfungen finden in unterschiedlichen Sektoren statt und sind aus Unternehmensperspektive bei der Minimierung von Geschäftsrisiken zentral, um das Risiko von Zahlungsausfällen von Kund:innen zu reduzieren. Im Telekommunikationssektor sind solche Prüfungen besonders relevant, wenn beim Abschluss von Mobilfunkverträgen Hardware an Kund:innen übergeben wird. Banken hingegen nutzen Bonitätsprüfungen vor allem im Vorfeld einer Kreditvergabe. Auch im Energiesektor gewinnen Bonitätsprüfungen zunehmend an Bedeutung und werden von Wirtschaftsauskunfteien für Energieversorger angeboten.[104]

Ein Problem bei der Bonitätsprüfung ist die Intransparenz der verwendeten Bewertungsmethoden. Die Algorithmen, die zur Berechnung von Kredit-Scores verwendet werden, können auf Daten basieren, die nicht vollständig oder repräsentativ sind.[105] Auf dieser Basis können bestimmte Gruppen von Konsument:innen benachteiligt werden, weil sie einer bestimmten Berufsgruppe angehören[106] oder weil sie keine umfassende Kreditgeschichte haben. Systeme zur Bonitätsprüfung können in weiterer Folge dazu führen, dass (eigentlich) kreditwürdige Antragsteller:innen abgelehnt werden oder höhere Tarifangebote erhalten.[107]

#### 5.3.3.1 Beispielhafter Ablauf der Bonitätsprüfung

Eine Bonitätsprüfung beginnt, wenn ein Kunde bzw eine Kundin (im Folgenden: Person) einen Kreditantrag stellt oder einen Vertrag abschließen möchte, bei dem das Unternehmen in Vorleistung tritt. Die Person gibt persönliche und finanzielle Informationen an, wie Einkommensnachweise und bestehende Schulden. Der Kreditgeber holt dann Informationen von Wirtschaftsauskunfteien, die Daten zu Krediten und Zahlungsausfällen (insb basierend auf § 152 GewO[108]) erheben. Alternativ kann die Bonitätsprüfung eigenständig durch das Unternehmen, basierend auf der eigenen Leistungserbringung oder Daten, die auch Auskunfteien nach § 152 GewO zur Verfügung stehen, erstellt werden. Diese Informationen werden zusammen mit weiteren Faktoren wie dem Einkommen und der Beschäftigung des Antragstellers analysiert. Auf Basis dieser Daten wird ein Bonitätsscore berechnet, der das Risiko eines Zahlungsausfalls bewertet. Der Kreditgeber trifft anschließend eine Entscheidung über den Antrag, die von der Bonität der Person abhängt. Bei Kreditvergabe werden über den Rückzahlungszeitraum Daten an die Wirtschaftsauskunftei rückgemeldet.[109]

---

[104] *CRIF*, Energie- & Versorgungsunternehmen, https://www.crif.at/fuer-unternehmen/branchen/energie-versorgungsunternehmen/ (abgerufen am 14. 2. 2025)
[105] *Chopra*, Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies, Vanderbilt Journal of Entertainment and Technology Law 2021, 625 (628 ff).
[106] *Centaurus Media Ltd*, Bonität und Berufswahl. Einflussfaktoren, https://www.sberbankdirect.de/bonitaet-und-berufswahl-einflussfaktoren/ (abgerufen am 29. 1. 2025)
[107] eag, Do Energy Suppliers Credit Score Organisations? https://eaguk.org/do-energy-suppliers-credit-score-organisations/ (abgerufen am 14. 2. 2025)
[108] Gewerbeordnung 1994 – GewO 1994, BGBl 194/1994 idF BGBl I 150/2024.
[109] *Oberwalder*, Bonitätsdatenbanken und deren datenschutzrechtliche Implikationen im Lichte des Verbraucherkreditgesetzes. Diplomarbeit Karl-Franzens-Universität Graz (2011).

#### 5.3.3.2 Rechtliche Beurteilung

Bei der Bonitätsprüfung werden grundsätzlich personenbezogene Daten verarbeitet, wodurch der Anwendungsbereich der DSGVO eröffnet ist und eine Rechtsgrundlage für die Datenverarbeitung nach Art 6 Abs 1 DSGVO erforderlich ist (sofern sensible Daten vorliegen, muss zusätzlich eine Rechtsgrundlage nach Art 9 Abs 2 DSGVO vorliegen). Der EuGH erkennt im Rahmen des Art 6 Abs 1 lit f DSGVO grundsätzlich ein berechtigtes Interesse an Datenverarbeitungen im Zusammenhang mit Bonitätsauskünften an.[110] Teilweise besteht auch eine Rechtspflicht zur Bonitätsprüfung (zB § 7 VKrG).[111] Das bedeutet aber nicht, dass jede Bewertungsmethodik auf Art 6 Abs 1 lit f DSGVO gestützt werden kann. Der EuGH fordert eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen, die grundsätzlich von den konkreten Umständen des Einzelfalls abhängt.[112] Das zweckentsprechende Interesse des Kreditors bzw der Auskunftei ist, bei Betrachtung der Eingriffstiefe der Datenverarbeitung, mit den Interessen des Betroffenen im Rahmen der Interessenabwägung abzuwägen. Die Eingriffstiefe wird etwa durch den Zeitraum der herangezogenen Daten oder deren Sensibilität (zB Gesundheitsdaten) determiniert.

Die Ermittlung der Bonität könnte sowohl unter Art 86 iVm Anhang III Z 5 lit b AI Act als auch Art 22 und 15 Abs 1 lit h DSGVO fallen. Aus Sicht des AI Act gilt es dazu zunächst zu prüfen, ob es sich um ein Hochrisiko-KI-System gemäß Art 6 Abs 2 iVm Anhang III handelt. Systeme, die zur Bewertung der Bonität oder Kreditwürdigkeit natürlicher Personen verwendet werden, gelten grds als hochriskant, da sie gravierende Auswirkungen auf die Lebensgrundlage haben können.[113] Dies greift der AI Act auch außerhalb der Erwägungsgründe auf, indem er KI-Systeme zur Bonitätsbewertung und Kreditwürdigkeitsprüfung in Anhang III Z 5 lit b ausdrücklich als Hochrisiko-KI-Systeme anführt, mit Ausnahme von KI-Systemen zur Aufdeckung von Finanzbetrug. Die Einordnung dieses Fallbeispiels unter Art 22 DSGVO, woran sich der Auskunftsanspruch nach Art 15 Abs 1 lit h DSGVO knüpft, wird in Abschnitt 5.4.1., der die Voraussetzungen des Art 22 DSGVO näher behandelt, noch einmal aufgegriffen.

[110] EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 79.
[111] Bundesgesetz über Verbraucherkreditverträge und andere Formen der Kreditierung zu Gunsten von Verbrauchern (Verbraucherkreditgesetz – VKrG), BGBl I 28/2010 idF BGBl I 1/2021.
[112] EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 83.
[113] Vgl ErwGr 58 AI Act.

### 5.3.4 Emotionserkennung im Marketing bzw zur Absatzförderung (Use Case 4)

Algorithmen zur Emotionserkennung bzw -verarbeitung, mitunter auch als *Affective Computing* behandelt, haben ein breites Anwendungsfeld. Dies betrifft auch das Marketing, etwa indem damit der Effekt von Werbung verbessert werden kann oder die Art und Weise, wie Personen auf bestimmte Produkte reagieren, genutzt wird, um Anpassungen bzw Verbesserungen an jenen Produkten vorzunehmen oder schlicht zu eruieren, wie diese ankommen. Es könnten dadurch aber auch direkt Kaufentscheidungen beeinflusst werden.[114]

Insbesondere aus der Perspektive datenschutzrechtlicher und KI-spezifischer Regelungen sind dabei verschiedene Konstellationen und Situationen denkbar, wobei einige mögliche Praxisbeispiele als Unterfälle dieses Use Cases Emotionserkennung herausgegriffen und diskutiert werden sollen:

1. Einsatz von Gestenerkennung zur Feststellung von Reaktionen in der Sportwettenwerbung zu deren Effizienzsteigerung (Use Case 4.1)
2. Einsatz von Emotionserkennung anhand von Aufnahmen des Gesichtsbereichs im Rahmen der Überprüfung der Identität (etwa bei Flugbuchungen), wobei auf erkannte Emotionen entsprechend reagiert wird (zB mittels sinkender Preise), um die Wahrscheinlichkeit für einen Kauf zu erhöhen (Use Case 4.2)
3. Einsatz von Emotionserkennung im Marketing für Waren oder Dienstleistungen, um zu erkennen, inwieweit diese angepasst werden könnten, etwa um die Zufriedenheit von Kund:innen zu erhöhen (Use Case 4.3);
    a. Unterfall 1: Anpassung von Reiseangeboten anhand emotionaler Reaktionen auf entsprechende Werbevideos, um möglichen individuellen Vorlieben besser zu entsprechen[115] (Use Case 4.3.a);
    b. Unterfall 2: Emotionsableitung auf der Basis von Texten oder Audiofiles von Stimmaufnahmen, um die Zufriedenheit von Bestandskund:innen zu analysieren und darauf zu reagieren[116] (Use Case 4.3.b)

[114] Siehe insgesamt *Dejam*, Gefühlsdatenschutz. Eine Untersuchung der datenschutzrechtlichen Rahmenbedingungen von Datenverarbeitungen mittels Affective Computing (2023) 37, 59 f, zu sonstigen Anwendungsbereichen generell auch 50 ff.
[115] Vgl *Prange*, Datenschutz- und lauterkeitsrechtliche Kernfragen des Einsatzes Künstlicher Intelligenz im Marketing, WRP 2024, 151 (Rz 22 ff).
[116] Vgl hierzu auch eine Entscheidung der ungarischen Datenschutzbehörde im Zusammenhang mit vergleichbaren Tätigkeiten einer Bank: NAIH 8. 2. 2022, NAIH-85-3/2022; siehe hierzu auch *Manso-Sayao*, NAIH (Hungary) - NAIH-85-3/2022, https://gdprhub.eu/NAIH_(Hungary)_-_NAIH-85-3/2022#Holding (Stand 28. 2. 2023).

#### 5.3.4.1 Datenbasis und Einordnung gemäß DSGVO und AI Act

Die Analyse von Emotionen erfordert zunächst gewisse Daten als Ausgangspunkt und kann dabei etwa auf Aufzeichnungen der Stimme, Videomitschnitten oder erfassten Körpersignalen wie Gehirnströmen basieren.[117] Bei der Verarbeitung von Daten über menschliche Gefühle handelt es sich in weiterer Folge idR – sofern keine Anonymisierung erfolgt – um eine Verarbeitung personenbezogener Daten im Sinne der DSGVO.[118]

Auch im Kontext von Werbung ist dabei je nach Form der Erhebung bzw Verarbeitung von Daten nicht ganz ausgeschlossen – wenn auch unwahrscheinlich – dass es sich um Gesundheitsdaten im Sinne von besonderen Kategorien personenbezogener Daten gemäß Art 9 DSGVO handelt. Diese wäre beispielsweise der Fall, sobald die Daten einen gesundheitsspezifischen Informationsgehalt (insbesondere über den gesundheitlichen Geisteszustand) beinhalten.[119]

Fraglich ist allerdings die Einordnung von durch Emotionserkennungssysteme verarbeiteten Daten als **biometrische Daten**, vor allem weil die DSGVO und der AI Act hierbei ein leicht unterschiedliches Verständnis haben dürften bzw sich zu widersprechen scheinen. Dies ist insbesondere deswegen relevant, weil sich demnach die Frage stellt, inwieweit für die Anwendbarkeit einschlägiger Regelungen des AI Act eine Verarbeitung sensibler Datenkategorien im Sinne der DSGVO (Art 9) erforderlich ist bzw ob nicht umgekehrt durch entsprechende Definitionen des AI Act sämtliche durch einschlägige Emotionserkennungssysteme verarbeitete Daten nunmehr als sensible Daten gem Art 9 DSGVO anzusehen sind.

In diesem Zusammenhang ist zunächst ErwGr 14 AI Act zu nennen, der festhält, dass biometrische Daten, was demnach auch im Rahmen des AI Act wie im Sinne der DSGVO[120] auszulegen wäre, „die Authentifizierung, Identifizierung oder Kategorisierung natürlicher Personen und die Erkennung von Emotionen natürlicher Personen ermöglichen [können]“.[121] Die Einordnung von bei der Emotionserkennung verwendeten Daten als biometrische Daten (insbesondere im Sinne der DSGVO) scheint in der Literatur allerdings vor der Gesetzwerdung des AI Act zumindest fraglich gewesen zu sein.[122] Dies wirkt alleine im Hinblick auf das von der Definition in Art 4 Z 14 DSGVO geforderte Merkmal, dass biometrische Daten „die

[117] Siehe *Dejam*, Gefühlsdatenschutz 45; vgl grundlegend auch *Gremsl/Hödl*, Emotional AI. Legal and ethical challenges, Information Polity 2022, 163 (163, 165).
[118] Siehe *Dejam*, Gefühlsdatenschutz 79, 83.
[119] Vgl *Dejam*, Gefühlsdatenschutz 252 ff; in Hinblick auf psychische Gesundheit (bzw derartige Daten) und entsprechende Anwendungen vgl grundlegend auch *Steindl*, Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in light of the Draft AI Act and its Interplay with the GDPR, European Data Protection Law Review 2022, 311 (312 f, 317).
[120] Expressis verbis im Sinne von “Artikel 4 Nummer 14 der Verordnung (EU) 2016/679, Artikel 3 Nummer 18 der Verordnung (EU) 2018/1725 und Artikel 3 Nummer 13 der Richtlinie (EU) 2016/680“.
[121] Zur Behandlung von Biometrie im AI Act und in diesem Zusammenhang auch zu Emotionserkennungssystemen vgl darüber hinaus ErwGr 54 AI Act.
[122] Keine Einordnung als *biometrische Daten* im Sinne der DSGVO etwa *Dejam*, Gefühlsdatenschutz 259; im Hinblick auf die dabei analysierte “*Facial Emotion Recognition*“ die Verarbeitung *biometrischer Daten* gem der DSGVO tendenziell relativ umfassend bejahend jedoch etwa auch: *Gremsl/Hödl*, Information Polity 2022, 163 (165 f); zur Diskussion einer Anpassung oder Neufassung/Aufteilung des rigiden Begriffsverständnisses *biometrischer Daten* gem DSGVO in Bezug auf den AI Act im Zusammenhang mit einem früheren Stadium des Gesetzgebungsverfahrens vgl auch *Steindl*, European Data Protection Law Review 2022, 311 (312 ff).

eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen“, nachvollziehbar, weil dies bei der Emotionserkennung schließlich nicht unbedingt der Fall sein müsste.[123]

Weiters definiert nunmehr auch Art 3 Z 34 AI Act biometrische Daten, und zwar als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische Daten“ und damit de facto identisch wie Art 4 Z 14 DSGVO mit eben jenem Unterschied, dass keine Ermöglichung oder Bestätigung der eindeutigen Identifizierung der betroffenen Person gefordert wird. Es scheint demnach einen gewissen Widerspruch zwischen dem Verständnis biometrischer Daten im Rahmen des AI Act (bzw in dessen Erwägungsgründen) und jenem der DSGVO zu geben. Hintergrund dessen ist, dass der Vorschlag zum AI Act ursprünglich eine mit Art 4 Z 14 DSGVO gänzlich **identische** Definition vorgesehen hatte (vormals Art 3 Z 33), das Merkmal der Ermöglichung oder Bestätigung der eindeutigen Identifizierung jedoch im Laufe des Gesetzgebungsverfahrens entfallen ist, während ErwGr 14 (vormals ErwGr 7) insbesondere um die Feststellung ergänzt wurde, dass durch solche Daten „die Authentifizierung, Identifizierung oder Kategorisierung natürlicher Personen und die Erkennung von Emotionen natürlicher Personen“ ermöglicht werden könne. Die Klarstellungen dazu, inwieweit die Definitionen der beiden Verordnungen für biometrische Daten miteinander verwandt sind, blieben zwar ähnlich. Es wird nunmehr jedoch nicht mehr davon gesprochen, dass die Begriffe „im Einklang“ miteinander stünden (und dementsprechend auszulegen wären), sondern eben lediglich noch davon, dass der AI Act-Begriff im Sinne des DSGVO-Begriffs ausgelegt werden sollte.[124]

#### 5.3.4.2 Biometrischer Daten gem AI Act auch maßgeblich für DSGVO?

Prinzipiell können bzgl der erläuterten Problemstellung verschiedene Überlegungen angestellt werden. Zunächst könnte argumentiert werden, dass durch den AI Act (auch) das Begriffsverständnis der DSGVO von biometrischen Daten dahingehend angepasst wurde, dass davon (quasi zusätzlich, unabhängig von der Ermöglichung oder Bestätigung der eindeutigen Identifizierung) insbesondere auch jene Daten, aus denen Emotionen abgeleitet werden können, erfasst wären.

Dagegen sprechen allerdings mehrere Argumente, denn die Auslegung des Begriffs biometrischer Daten im Sinne des AI Acts und insbesondere der zitierten Erläuterungen in ErwGr 14 AI Act scheint **im Regime der DSGVO** zunächst *contra verbis legis* zu sein, weil diese für das Vorliegen biometrischer Daten gem Art 4 Z 14 leg cit eben die **Ermöglichung oder Bestätigung der eindeutigen Identifizierung betroffener Personen** verlangt. Hierzu ist zunächst festzustellen, dass deren Begriffsverständnis durch einen ErwGr in einer anderen

[123] Vgl erneut *Steindl*, European Data Protection Law Review 2022, 311 (314 f); *Dejam*, Gefühlsdatenschutz 259.
[124] Vgl zu alledem auch *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 3 Rz 228 ff, vor allem Rz 232 ff; und insbesondere die Feststellungen, dass im Rahmen der DSGVO auf einen engeren Kreis biometrischer Daten abgezielt wird, was im Hinblick auf den AI Act als unpassend erachtet wurde, weshalb in der Folge verschiedene Lösungsmöglichkeiten verhandelt wurden, wobei nun ein gewisser Widerspruch entstanden ist.

Verordnung alleine wohl nicht derart erweitert werden könnte.[125] Lediglich in Verbindung mit der breiteren Fassung von Art 3 Z 34 AI Act gegenüber Art 4 Z 14 DSGVO könnte eine weitere Interpretation des DSGVO-Begriffs nahegelegt werden. Ein starkes Gegenargument hierzu ist aber Folgendes: Zwar wurde auch der AI Act, wie die DSGVO, auf Basis des AEUV, und zwar in dem Zusammenhang insbesondere Art 16, durch das Europäische Parlament und den Rat der EU auf Vorschlag der EU-Kommission im ordentlichen Gesetzgebungsverfahren erlassen. Jedoch wurde zum einen explizit in Art 2 Abs 7 AI Act festgehalten, dass dieser prinzipiell[126] „nicht die Verordnung (EU) 2016/679 bzw (EU) 2018/1725 oder die Richtlinie 2002/58/EG bzw (EU) 2016/680 [berührt]" bzw dass „[d]ie Rechtsvorschriften der Union zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation […] für die Verarbeitung personenbezogener Daten im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten [gelten]". Demnach sollte die DSGVO prinzipiell unverändert bleiben.

Weiters ist die oben dargelegte Anpassung des ErwGr 14 AI Act wohl derart zu deuten, dass die AI Act-Definition biometrischer Daten nur soweit wie jene der DSGVO auszulegen ist, **als sich diese tatsächlich entsprechen** (arg: Auslegung „im Sinne des Begriffs" der DSGVO und nicht mehr „im Einklang" miteinander).[127] Dementsprechend scheint im Ergebnis auch ErwGr 14 AI Act gegen eine Ausdehnung des DSGVO-Verständnisses biometrischer Daten zu sprechen, indem dieser lediglich auf eine **sinnentsprechende** (und keine identische) Auslegung des AI Act-Begriffs abzielen dürfte.

*Wendehorst* argumentiert in diesem Zusammenhang, dass das Begriffsverständnis von Art 4 Z 14 DSGVO in der Theorie insoweit gedehnt werden könnte, als jedes biometrische Merkmal auch dafür verwendet werden könnte, die Identität der betroffenen Person zu **bestätigen**, auch wenn dies in der Praxis in Bezug auf Ungenauigkeiten dabei unzweckmäßig wäre. Gleichzeitig wird dabei darauf verwiesen, dass Art 9 Abs 1 DSGVO weiterhin nur biometrische Daten „zur eindeutigen Identifizierung einer natürlichen Person" adressiert, wodurch sich im Hinblick auf wesentliche Anknüpfungen an diese Bestimmung (und nicht an die Definition biometrischer Daten) im Ergebnis ohnehin wenig ändern würde.[128]

#### 5.3.4.3 Biometrischer Daten gem DSGVO auch maßgeblich für AI Act?

Auf Basis der Voraussetzung biometrischer Daten für die Definition von

[125] Siehe MwN EuGH 21. 4. 2023, C-10/23, *Remia Com Impex*, ECLI:EU:C:2024:259, Rz 51: „Nach ständiger Rechtsprechung können die Erwägungsgründe eines Unionsrechtsakts den Inhalt seiner Bestimmungen präzisieren und sind ein wichtiges Auslegungselement, das den Willen des Gesetzgebers erhellen kann […]" und insbesondere EuGH 13. 7. 2023, C-376/20 P, *Kommission/CK Telecoms UK Investments,* ECLI:EU:C:2023:561, Rz 105 mwN: „Die Erwägungsgründe eines Unionsrechtsakts sind jedoch rechtlich nicht verbindlich und können weder herangezogen werden, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht […]."

[126] Nämlich „unbeschadet des Artikels 10 Absatz 5 und des Artikels 59 der vorliegenden Verordnung".

[127] Schließlich wurde die Klarstellung gestrichen, dass sich die Definitionen im Einklang befänden (und dementsprechend auszulegen wären), und dadurch ersetzt, dass der AI-Act-Begriff **im Sinne** jenes der DSGVO auszulegen wäre.

[128] Siehe im Detail *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 247.

Emotionserkennungssystemen in Art 3 Z 39 AI Act (siehe schon 5.2.2) könnte zudem überlegt werden, ob die Regelungen nicht schlicht so zu verstehen sind, dass nur jene Systeme vom AI Act erfasst sein sollen, die auch Daten verarbeiten, die Art 4 Z 14 DSGVO entsprechend eine eindeutige Identifizierung von natürlichen Personen (und **darüber hinaus** eben eine Feststellung oder Ableitung von Emotionen) ermöglichen bzw bestätigen. Demnach wäre noch einmal konkreter zu hinterfragen, inwieweit das Begriffsverständnis der DSGVO für biometrische Daten für jenes des AI Act maßgeblich ist.[129] Allein im Hinblick auf die Formulierung von ErwGr 14 AI Act erscheint diese Interpretation bis zu einem gewissen Grad denkmöglich,[130] wäre allerdings der kritischen Literatur folgend (siehe oben), zunächst eine deutliche Einschränkung jenes Aspekts des Anwendungsbereichs der Regelungen und scheint vor allem der nunmehr weiteren Definition biometrischer Daten in Art 3 Z 34 AI Act zu widersprechen, zumal das Merkmal der Voraussetzung der Ermöglichung oder Bestätigung der eindeutigen Identifizierung erst im Laufe des Gesetzgebungsverfahrens entfallen ist, was schließlich eine entsprechende Absicht verdeutlicht[131]. Unterstrichen wird dies auch durch die oben zitierte Änderung in ErwGr 14 AI Act, wobei die Aussage, dass die beiden Begriffe „im Einklang“ miteinander stünden (und dementsprechend auszulegen wären), darauf abgeändert wurde, dass der AI Act-Begriff im Sinne des DSGVO-Begriffs ausgelegt werden sollte, was wie bereits dargelegt eine Abschwächung der gemeinsamen Interpretierbarkeit nahelegt.[132]

#### 5.3.4.4 Fazit zu Begrifflichkeiten biometrischer Daten

Aus alledem folgt, dass der potenzielle Widerspruch der Definitionen wohl so aufzulösen ist, dass der **im Rahmen des AI Act** verwendete Begriff biometrischer Daten mit Ausnahme der Voraussetzung der Ermöglichung oder Bestätigung der eindeutigen Identifizierung wie Art 4 Z 14 DSGVO zu verstehen ist.[133] Dies könnte wohl unter anderem mit der entsprechenden Ergänzung in ErwGr 14 AI Act erfolgen, dass diese Daten insbesondere auch „die Erkennung von Emotionen natürlicher Personen ermöglichen“ können, weil dies der weiteren Formulierung des AI Act zu entsprechen scheint. Dieser weiteren AI Act-Definition folgend sind jene in ErwGr 14 AI Act angeführten Merkmale biometrischer Daten demnach wohl eher als mehrere Möglichkeiten denn als kumulative Eigenschaften zu verstehen (zB: Ermöglichung der Identifizierung **oder** der Emotionserkennung durch entsprechende Daten).[134]

---

[129] Vgl erneut etwa *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 89 (Rz 90).

[130] Vgl insbesondere die Formulierung “Der in dieser Verordnung verwendete Begriff ‘biometrische Daten’ sollte im Sinne des Begriffs ‘biometrische Daten’ nach [...] [der DSGVO] ausgelegt werden“ (Anmerkung: Anführungszeichen angepasst).

[131] Vgl dazu erneut auch *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 232 ff und 245 ff.

[132] Im Übrigen wären mit derartigen Überlegungen allein auch die Auswirkungen auf das Begriffsverständnis *biometrischer Daten* nach der DSGVO noch nicht restlos geklärt. Immerhin wären – gewissermaßen umgekehrt zu den obigen Überlegungen – wohl auch nicht alle Arten biometrischer Daten im Sinne von Art 4 Z 14 DSGVO dazu geeignet, daraus Emotionen abzuleiten (vgl etwa Fingerabdrücke zur eindeutigen Identifizierung: siehe dazu etwa *Hödl* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 4 DSGVO Rz 148 f mwN [Stand 1. 12. 2018, rdb.at]).

[133] Vgl im Ergebnis wohl ähnlich *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 228 ff; in diesem Sinne auch *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 89 (Rz 90) bzw *Hansen/Nägele/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 165 (Rz 165).

[134] Dies würde gewissermaßen auch von ErwGr 18 AI Act gestützt werden, der im Hinblick auf

Zusammenfassend kann daher festgehalten werden, dass das Begriffsverständnis des AI Act von biometrischen Daten und dessen Verhältnis zu jenem der DSGVO derzeit noch bis zu einem gewissen Grad unklar ist. Unter dem Strich verhält es sich aber wohl so, dass die DSGVO (nach wie vor) für die Definition biometrischer Daten verlangt, dass diese die eindeutige Identifizierung der betroffenen Person ermöglichen oder bestätigen. Selbst wenn diese Begriffsdefinition im Lichte des AI Acts möglichst weit ausgelegt würde, bezieht sich Art 9 Abs 1 DSGVO *Wendehorst* folgend immer noch auf biometrische Daten „**zur eindeutigen Identifizierung**" natürlicher Personen, was unter dem Strich jedenfalls eine entsprechende Beschränkung wesentlicher Regelungen bedeuten wird. Der AI Act verlangt derartiges für dessen Definition biometrischer Daten demgegenüber wohl **nicht**. Die Definition des AI Act soll neben Daten, die die Authentifizierung, Identifizierung oder Kategorisierung natürlicher Personen ermöglichen, auch solche, die die Erkennung von Emotionen natürlicher Personen ermöglichen, umfassen, ist aber prinzipiell bzw ansonsten wohl wie die Definition nach der DSGVO auszulegen.[135] *Wendehorst* hält in dem Zusammenhang fest, dass man im Hinblick auf den AI Act schlussendlich darauf abstellen wird müssen, ob die Verarbeitung der Daten mittels spezieller technischer Mittel so erfolgt, dass damit vorrangige Funktionen von Biometrieverfahren umgesetzt werden können, worunter auch die entsprechende Merkmalserkennung und damit auch die Emotionserkennung fallen würde.[136]

Jedenfalls setzt das Begriffsverständnis des AI Act für Emotionserkennungssysteme aber voraus, dass dabei personenbezogene Daten verwendet werden[137], sowie nach *Wendehorst* wohl im Wesentlichen, dass es sich um Daten handelt, die mit speziellen technischen Mitteln für die Emotionserkennung durch das Messen biologischer Signale im Hinblick auf bestimmte Personenmerkmale gewonnen werden[138], was auch bereits eine gewisse Einschränkung bedeutet[139].

Nach *Wendehorst* sind dabei biometrische Inferenzen, also Ableitungen von physischen, physiologischen oder verhaltenstypischen Merkmalen aus generellen personenbezogenen Daten, tendenziell nicht erfasst.[140] Im Hinblick auf die geforderten physischen, physiologischen oder verhaltenstypischen Merkmale hält dieselbe fest, dass diese in verschiedenartig eingeteilt werden können und dass im Speziellen schwache biometrische Merkmale (zB Körpersignale, Gang oder Interaktionen mit Maschinen), die nicht so eindeutig sind wie etwa ein

*Emotionserkennungssysteme* von der Erkennung von Ausdrucksformen wie etwa Handbewegungen spricht; aus solchen Gesten alleine müsste sich schließlich wohl noch keine eindeutige Identifizierbarkeit ergeben (vgl auch die obigen Überlegungen sowie jene der Literatur iZm der DSGVO).

[135] Grundlegend in diesem Sinne auch *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 89 (Rz 90) bzw *Hansen/Nägele/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 165 (Rz 165).

[136] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 KI-VO Rz 245.

[137] Vgl insbesondere die Definitionen in Art 3 Z 34 und 39 AI Act (siehe auch noch unten) und ErwGr 14; siehe auch *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 236 f.

[138] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 238 ff, 243 ff.

[139] Vgl zudem *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 280.

[140] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 246; vgl auch Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, grundlegend ähnlich unter 7.4, hingegen werden unter 7.2.1. b) Ableitungen, die nicht ausschließlich auf den Daten beruhen, die über die betroffene Person erhoben wurden, scheinbar schon als erfasst gesehen.

Fingerabdruck als starkes biometrisches Merkmal, vor allem für Emotionserkennung bzw im Rahmen von gezieltem Marketing genutzt werden können.[141]

#### 5.3.4.5 Einordnung von Emotionserkennungssystemen gem AI Act

Im Hinblick auf entsprechende Algorithmen bzw Systeme und die Anwendung des AI Act im Allgemeinen wäre jedoch zunächst zu eruieren, inwieweit ein erfasstes „*KI-System*“ vorliegt. Siehe dazu im Detail bereits Kapitel 5.2.2.

Sofern dies der Fall ist, stellt sich insbesondere die Frage, in welche der Risikostufen, die sich aus dem AI Act ergeben (siehe ebenso Kapitel 5.2.2), ein solches KI-System einzuordnen wäre. Dabei ist erneut anzumerken, dass der AI Act zusätzlich zur allgemeinen Definition von KI-Systemen auch Emotionserkennungssysteme definiert (Art 3 Z 39), und zwar als „ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten“ (siehe auch schon Kapitel 5.2.2). ErwGr 18 AI Act hält dazu zudem fest, dass es bei dem Begriff „um Emotionen oder Absichten wie Glück, Trauer, Wut, Überraschung, Ekel, Verlegenheit, Aufregung, Scham, Verachtung, Zufriedenheit und Vergnügen“ ginge und wiederum „nicht physische Zustände wie Schmerz oder Ermüdung, einschließlich beispielsweise Systeme, die zur Erkennung des Zustands der Ermüdung von Berufspiloten oder -fahrern eingesetzt [Anm: Fehler berichtigt] werden, um Unfälle zu verhindern“ erfasst sein sollten. Weiters wird darin festgestellt, dass damit nicht „die bloße Erkennung offensichtlicher Ausdrucksformen, Gesten und Bewegungen“ adressiert werde, sofern diese nicht „zum Erkennen oder Ableiten von Emotionen verwendet“ würden. Angemerkt wird dazu ferner noch: „Bei diesen Ausdrucksformen kann es sich um einfache Gesichtsausdrücke wie ein Stirnrunzeln oder ein Lächeln oder um Gesten wie Hand-, Arm- oder Kopfbewegungen oder um die Stimmmerkmale einer Person handeln, wie eine erhobene Stimme oder ein Flüstern“.

Für Absichten (auf deren Ableitung oder Erkennung die Definition abzielt) wäre nach *Wendehorst* wohl auf eine direkte Ableitbarkeit aus biometrischen Daten abzustellen und dabei zB die Absicht, einen spezifischen Kauf abzuschließen, was sich etwa aus Augenbewegungen oder Haltungsänderungen ergeben könne, zu nennen.[142]

In weiterer Folge verbietet zunächst Art 5 Abs 1 lit f AI Act „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am **Arbeitsplatz und in Bildungseinrichtungen**, **es sei denn**, die Verwendung des KI-Systems soll **aus medizinischen Gründen oder Sicherheitsgründen** eingeführt oder auf den Markt gebracht werden“[143]. Grundlegend enthält ErwGr 44 AI Act hierzu Erläuterungen zum Hintergrund bzw zu den dahinter liegenden Absichten. Außerdem ist anzumerken, dass bei diesem Verbot der Begriff „Emotionserkennungssystem“ vermieden wird, was gewisse Implikationen im Hinblick

[141] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 238 ff.
[142] Vgl insgesamt *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 282.
[143] Hervorhebungen hinzugefügt.

auf das bisher hierzu Ausgeführte bergen würde; insbesondere scheint Art 5 Abs 1 lit f AI Act (im Gegensatz zur Definition gem Art 3 Z 39) nur auf **Emotionen** und nicht auch auf **Absichten** abzustellen.[144] Zudem wird argumentiert, dass hierbei nicht unbedingt biometrische Daten im oben dargestellten Sinn als Ausgangsbasis erforderlich wären, sondern prinzipiell auch allgemeinere Datenkategorien dafür in Frage kämen.[145] Dieses Verbot ist im Zusammenhang mit Werbemaßnahmen demnach wohl wenig relevant, wenn auch nicht völlig irrelevant.

Weiters werden im Allgemeinen gem Art 6 Abs 2 AI Act prinzipiell jene KI-Systeme als Hochrisiko-Systeme eingestuft, die in Anhang III AI Act genannt werden[146], was nach Anhang III Ziffer 1 lit c auch solche KI-Systeme betrifft, „die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen".[147] Für diese gelten in weiterer Folge die meisten inhaltlichen Regelungen des AI Act. Unter gewissen Umständen können allerdings von Art 6 Abs 2 AI Act abweichende Einstufungen vorgenommen werden (vgl insgesamt bereits unter 5.2.2).

Jedenfalls unterliegen Betreiber von Emotionserkennungssystemen (bzw von Systemen zur biometrischen Kategorisierung) gewissen Transparenzverpflichtungen: Gemäß Art 50 Abs 3 AI Act haben diese prinzipiell „die davon betroffenen natürlichen Personen über den Betrieb des Systems" zu informieren.[148]

#### 5.3.4.6 Rechtliche Beurteilung

Im Hinblick auf die oben genannten Use Cases ergibt sich demnach folgendes erstes rechtliches Bild:

Zunächst werden wohl bei allen Varianten, etwa durch Videoaufnahmen des Gesichts einer Person, unter Berücksichtigung der obigen Ausführungen in aller Regel personenbezogene Daten im Sinne der DSGVO verarbeitet. Insbesondere im Fall der Verarbeitung ausreichend anonymer Daten, etwa durch Aggregierung von Daten, wäre dies uU nicht gegeben. Inwieweit es sich dabei zwingend auch um biometrische Daten im Sinne von Art 4 Z 14 bzw Art 9 Abs 1 DSGVO (und damit besondere Datenkategorien) handelt, ist der obigen Diskussion folgend bis zu einem gewissen Grad fraglich, im Ergebnis jedoch (zumindest hinsichtlich besonderer Datenkategorien gem Art 9 Abs 1 DSGVO) tendenziell regelmäßig zu verneinen.[149] In Use Case 4.2 werden demgegenüber in aller Regel wohl auch biometrische Daten gem Art 4 Z 14

[144] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 279 und im Detail *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 5 Rz 105 ff.
[145] Vgl im Detail *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 106 f; vgl insgesamt, mit scheinbar jeweils gegenteiliger Auslegung, auch: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (insbesondere 7.2.1. a), 7.4).
[146] Siehe im Detail, insbesondere auch zur Einstufung gemäß Art 6 Abs 1 AI Act, Kapitel 5.2.2.
[147] Vgl auch *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 279.
[148] Dabei sind „gesetzlich zur Aufdeckung, Verhütung oder Ermittlung von Straftaten zugelassene KI-Systeme, die zur biometrischen Kategorisierung und Emotionserkennung im Einklang mit dem Unionsrecht verwendet werden, sofern geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen" ausgenommen.
[149] Und zwar insbesondere mit dem Argument, dass zumindest Art 9 Abs 1 DSGVO unverändert "Daten zur eindeutigen Identifizierung einer natürlichen Person" erfordert; vgl hierzu im Detail die obigen Ausführungen.

bzw Art 9 Abs 1 DSGVO vorliegen.

In Bezug auf den AI Act müssten die dabei eingesetzten Systeme zunächst die allgemeine Definition für KI-Systeme gem Art 3 Z 1 erfüllen, was oftmals der Fall sein wird. Weiters stellt sich die Frage, ob ein Emotionserkennungssystem gem Art 3 Z 39 AI Act vorliegt, und dabei insbesondere, inwieweit dazu Daten verarbeitet werden müssen, die (auch) die eindeutige Identifizierung der betroffenen natürlichen Personen ermöglichen oder bestätigen (also inwieweit dabei Art 4 Z 14 DSGVO maßgeblich ist). Nach der hier vertretenen Ansicht ist Letzteres durch den AI Act wohl nicht bezweckt und demnach keine Ermöglichung oder Bestätigung der eindeutigen Identifizierung der betroffenen Person erforderlich (siehe im Detail oben). Jedenfalls aber müssten biometrische Daten im Sinne von Art 3 Z 34 AI Act vorliegen, und damit insbesondere „mit speziellen technischen Verfahren gewonnene personenbezogene Daten“ zu den „physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person“. Nach ErwGr 14 AI Act können diese Daten insbesondere auch „die Erkennung von Emotionen natürlicher Personen ermöglichen“.

Personenbezogene Daten, aus denen sich Emotionen ableiten lassen, würden demnach in der Regel bei allen drei genannten Use Cases vorliegen. Allerdings wäre dies (*Wendehorst* folgend) nur insoweit einschlägig, als diese Daten durch eine (direkte) Messung biologischer Signale zu entsprechenden Personenmerkmalen mittels spezieller technischer Mittel, die insbesondere auf einen solchen Emotionserkennungszweck abzielen, gewonnen werden (vgl im Detail oben). Dies muss freilich im jeweiligen einzelnen Anwendungsfall, insbesondere anhand der konkreten technischen Herangehensweise, geklärt werden. Im Hinblick auf die Use Cases wäre dies aber am ehesten bei Use Case 4.3.b im Allgemeinen fraglich, soweit lediglich Texte zur Ableitung etwaiger Emotionen verwendet würden, weil diesfalls wohl in der Regel keine direkte Messung biologischer Signale vorliegen würde.[150] Die entsprechende Analyse von Tastaturanschlägen im Sinne von Handbewegungen bzw Gesten, auf deren Basis Emotionen erkannt oder daraus abgeleitet werden (vgl ErwGr 18 AI Act) wäre in diesem Zusammenhang wiederum eindeutiger.[151]

In weiterer Folge stellt sich die Frage, ob durch das KI-System auf der entsprechenden Datenbasis Emotionen oder Absichten natürlicher Personen festgestellt oder daraus abgeleitet werden sollen. Im Hinblick auf Use Case 4.1 ist dabei insbesondere relevant, ob anhand von Gesten **emotionale** Reaktionen (bzw allenfalls Absichten, wie jene, eine Wette abzuschließen) erkannt werden sollen oder lediglich andere Gegebenheiten oder Zustände (vgl insbesondere die Präzisierungen in ErwGr 18 AI Act). Im Fall der anderen beiden Use Cases wäre dieser Aspekt wohl wiederum eindeutiger.

Als Betreiber von Emotionserkennungssystemen müssten entsprechende Akteure damit jedenfalls im Zuge der Transparenzverpflichtungen gem Art 50 Abs 3 AI Act „die davon betroffenen natürlichen Personen über den Betrieb des Systems“ informieren.[152] Diese

[150] Vgl zu diesem Aspekt erneut *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 246.
[151] Vgl dazu insgesamt auch *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 106; vgl zudem auch Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (insbesondere 7.2.1. c)).
[152] Die Ausnahme von „gesetzlich zur Aufdeckung, Verhütung oder Ermittlung von Straftaten zugelassene[n] KI-

Informationen müssen „den betreffenden natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt“ werden und „den geltenden Barrierefreiheitsanforderungen entsprechen“ (Art 50 Abs 5 AI Act).

Unabhängig davon (vgl Art 50 Abs 6 AI Act) stellt sich aber schließlich die Frage, in welche der Risikostufen des AI Acts entsprechende Systeme einzuordnen wären.

Zunächst könnten verbotene Systeme gem Art 5 AI Act vorliegen, sofern diese am Arbeitsplatz oder in Bildungseinrichtungen zu Zwecken des Marketings/der Absatzförderung eingesetzt würden (vgl Art 5 Abs 1 lit f AI Act), was nicht prinzipiell ausgeschlossen, aber eher unwahrscheinlich erscheint.

Insbesondere in Bezug auf Use Case 4.1 und den Einsatz von KI in der Sportwettenwerbung stellt sich etwa im Hinblick auf spielsüchtige Personen die Frage, inwieweit nicht eine verbotene Praktik gem Art 5 Abs 1 lit b AI Act vorliegen könnte. Bei der Bestimmung geht es um die Ausnützung der Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird. Demnach wäre im Zusammenhang mit Use Case 4.1 zunächst insbesondere relevant, ob das System die Vulnerabilität/Schutzbedürftigkeit von spielsüchtigen Personen mit der Wirkung (oder dem Ziel) ausnutzt, ihr Verhalten derart wesentlich zu ändern, dass ihr zumindest mit hinreichender Wahrscheinlichkeit ein erheblicher Schaden zugefügt wird.[153]

Nach dem Wortlaut müsste das System daher gewissermaßen gezielt auf den Umstand abzielen, der die Schutzbedürftigkeit begründet, was bei der schlichten Erkennung von Emotionen bei einem allgemeinen Adressatenkreis fraglich erscheint.[154] Dies könnte uE etwa relevant sein, wenn die Emotionserkennung lediglich dazu eingesetzt wird, bei einem allgemeinen Adressatenkreis Personen, die positiv reagieren, eine längere Werbeschaltung

---

Systeme[n], die zur biometrischen Kategorisierung und Emotionserkennung im Einklang mit dem Unionsrecht verwendet werden, sofern geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen“ wäre im gegebenen Zusammenhang naturgemäß wohl nicht relevant.

[153] Freilich könnten im Hinblick auf die verschiedenen Möglichkeiten der Bestimmung im Detail noch andere Konstellationen überlegt werden, die ausgeführte erscheint jedoch hinsichtlich des Sachverhalts als am relevantesten.

[154] Vgl neben dem Wortlaut von Art 5 Abs 1 lit b AI Act auch folgende Passage in ErwGr 29, wonach der manipulative bzw ausbeuterische Charakter der KI ein wesentliches Element zu sein scheint: “In jedem Fall ist es nicht erforderlich, dass der Anbieter oder der Betreiber die Absicht haben, erheblichen Schaden zuzufügen, wenn dieser Schaden aufgrund von manipulativen oder ausbeuterischen KI-gestützten Praktiken entsteht“; wenn aber in allgemeiner Manier lediglich die konkreten, aktuellen Emotionen potenzieller Kund*innen analysiert würden, erscheint es demnach fraglich, ob dabei schon spezifisch auf die Ausnützung der Schutzwürdigkeit bestimmter Personen abgezielt würde; vgl auch “However, Article 5(1)(b) AI Act does not apply to AI systems that target consumers based on a wide ranging variables that do not tangentially correlate with vulnerable groups in specific socio-economic situations, such as what brand and model of telephone a person has, in how big city they live, how much and where they travel etc. Even if these characteristics may reflect socio-economic situation [sic] of individuals in general, they are not determinative of individuals in a specific socio-economic situation, whose vulnerabilities the prohibition aims to safeguard against exploitation“: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).

zu zeigen als Personen, die negativ darauf reagieren. *Wendehorst* merkt in diesem Zusammenhang an, dass zwar eine entsprechende Ausnützungsabsicht hinsichtlich Verhaltensänderungen erforderlich wäre, eine solche aber vermutet würde, sofern objektiv betrachtet ein entsprechender Effekt eintritt, wobei die Beeinflussung gem ErwGr 29 AI Act quasi nicht aufgrund externer Gegebenheiten eintreten darf, die von den Verpflichteten nicht vernünftig antizipiert oder mitigiert werden könnten.[155] Im Hinblick auf Use Case 4.1 ist daher zu konstatieren, dass spielsüchtige Personen vermutlich auch durch eine entsprechende Emotionserkennung eher gefährdet wären als andere Personen, was in diesem Sinne zumindest mittelbar bzw effektiv eine (Aus-)Nutzung dieses schutzwürdigen Umstands denkbar erscheinen lässt.

Da für eine wesentliche Verhaltensänderung etwa schon längeres Verweilen in Social Media als geplant als ausreichend erachtet wird[156], kann wohl auch der Abschluss von Sportwetten oÄ entgegen der ursprünglichen Absicht der jeweiligen Person diesbezüglich einschlägig sein.

Weiters müsste insbesondere mit hinreichender Wahrscheinlichkeit ein erheblicher Schaden drohen. Nach ErwGr 29 AI Act kann es dabei auch um Schäden gehen, die sich im Laufe der Zeit anhäufen können, wodurch nicht jeder Schadenseintritt erheblich für sich sein muss.[157] Nach der Zielrichtung (nämlich vor allem der anvisierten Schutzgüter), der Systematik des AI Acts und der verbotenen Praktiken im Besonderen ist der Begriff Schaden wohl durchaus umfassend zu verstehen.[158] Nach *Wendehorst* sind Schäden jeder Art relevant.[159] Dabei stellt sich die Frage, ob allein durch (die Steigerung der Effizienz von) Werbung bereits mit hinreichender Wahrscheinlichkeit ein erheblicher Schaden bei betroffenen, insbesondere spielsüchtigen Personen entstehen muss. Je nach den Umständen des Einzelfalls erscheint aber die Erhöhung der Wahrscheinlichkeit von finanziellen oder psychischen Schäden für spielsüchtige Personen durch entsprechende Werbung durchaus denkbar.

Zu fragen wäre weiters, ob insbesondere spielsüchtige Personen per se schon einem von Art 5 Abs 1 lit b AI Act geschützten Personenkreis zugeordnet werden können, zumal die Aufzählung darin abschließend zu sein scheint[160]. Personen mit Spielsucht erscheinen zunächst weder allgemein aufgrund ihres Alters schutzwürdig, noch fallen diese wohl unbedingt unter eine bestimmte soziale oder wirtschaftliche Situation. Darunter versteht ErwGr 29 beispielsweise extreme Armut oder ethnische oder religiöse Minderheiten, wobei es generell um eine höhere Anfälligkeit für Ausnützungen gehen soll.[161] Nachdem Spielsucht per

[155] Siehe *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 56; vgl auch "'Exploitation' should be understood as objectively making use of such vulnerabilities [...]": Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).
[156] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 57.
[157] *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 45.
[158] Vgl insbesondere Art 1 Abs 1 und ErwGr 5 AI Act sowie zu den verbotenen Praktiken insbesondere auch ErwGr 29; vgl weiters etwa Art 27 AI Act zu Schadensrisiken im Zusammenhang mit Grundrechten, siehe dazu etwa *Fülöp/Poindl* in *Pehlivan/Forgó/Valcke*, The EU Artificial Intelligence (AI) Act. A Commentary (2024) Art 27 Abschnitt 3.2.2 und 3.3.4.4.
[159] Siehe *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 58.
[160] Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 53; Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (insb 3.3.1.).
[161] Siehe auch *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 55.

se wohl noch nicht zwangsläufig mit einer bestimmten wirtschaftlichen Situation einhergehen muss, müsste im Hinblick auf das Verbot wohl weniger auf die Spielsucht direkt abgestellt werden, als vielmehr darauf, ob sich die Person (wenn auch sogar aufgrund einer solchen Sucht) in einer wirtschaftlichen Zwangslage oder einer ähnlichen Situation befindet.[162] Dies erscheint jedoch im entsprechenden Zusammenhang grundsätzlich auch denkbar. Ein mögliches Beispiel wäre wohl, dass eine solche Zwangslage durch das KI-System erkannt wird bzw zumindest faktisch ein solcher Personenkreis anvisiert wird und der betroffenen Person suggeriert wird, dass sie mit Sportwetten schnell viel Geld verdienen kann, wodurch in der Folge ein erheblicher finanzieller Schaden entsprechend wahrscheinlich erscheint. Die entscheidende Funktion der KI läge dann aber wohl insbesondere darin, eine solche wirtschaftliche Zwangslage mehr oder weniger gezielt zu adressieren, wenngleich dies wohl auch unter Zuhilfenahme von Emotionserkennung erfolgen könnte. Dies könnte naturgemäß wiederum auch für andere Anwendungsfälle in der Werbung relevant sein. Zudem werden Personen mit Behinderungen basierend auf einer langfristigen körperlichen, seelischen, geistigen oder Sinnesbeeinträchtigung geschützt,[163] weshalb entsprechende Überlegungen vor allem auch auf dieser Basis unternommen werden könnten; insbesondere in Hinblick auf die Definition von Spielsucht als psychische Beeinträchtigung nach ICD-11 (Code 6C50).[164]

Etwa bei der pauschalen Verwendung (mit allgemeinem Adressatenkreis) von Emotionserkennung dazu, Personen, die positiv reagieren, eine längere Werbeschaltung zu zeigen, als Personen, die negativ darauf reagieren, erscheint das Verbot im Allgemeinen jedoch tendenziell unzutreffend.[165] ErwGr 29 AI Act hält in diesem Zusammenhang auch fest, dass „übliche und rechtmäßige Geschäftspraktiken, beispielsweise im Bereich der Werbung, die im Einklang mit den geltenden Rechtsvorschriften stehen, als solche nicht als schädliche manipulative KI-gestützten Praktiken gelten“ sollten.[166] Von Emotionserkennung gestützte Werbung wird zwar wohl (noch) nicht unbedingt als üblich zu erachten sein. Nichtsdestotrotz scheinen pauschale Werbepraktiken auch nicht unbedingt tatbestandsmäßig einen Nutzen aus entsprechenden Vulnerabilitäten zu ziehen. Ansonsten könnte dies freilich auch auf andere Anwendungsfälle in der Werbung zutreffen (wie etwa Use Case 4.3.a), bei denen

[162] Vgl auch “5(1)(b) AI Act aims to ensure that AI technologies do not perpetuate or exacerbate existing financial and other social inequalities and injustices by exploiting the vulnerabilities of those people“ sowie “For example, an AI-predictive algorithm can be used to target with advertisements for predatory financial products people who live in low-income post-codes and are in a dire financial situation, thus exploiting their susceptibility to such advertisements because of possible despair and causing them significant financial harm“: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).
[163] *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 Rz 54.
[164] Vgl https://icd.who.int/browse/2025-01/mms/en#960730313 (abgerufen am 17. 2. 2024).
[165] Vgl allgemein auch “However, Article 5(1)(b) AI Act does not apply to AI systems that target consumers based on a wide ranging variables that do not tangentially correlate with vulnerable groups in specific socio-economic situations, such as what brand and model of telephone a person has, in how big city they live, how much and where they travel etc. Even if these characteristics may reflect socio-economic situation [sic] of individuals in general, they are not determinative of individuals in a specific socio-economic situation, whose vulnerabilities the prohibition aims to safeguard against exploitation“: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).
[166] Dazu ist anzumerken, dass freilich auch nach anderen (nationalen) Vorschriften entsprechende Beschränkungen möglich sind.

Personen in wirtschaftlich prekären Situationen uU stärker negativ betroffen wären. Den obigen Ausführungen entsprechend ist dies aber in Bereichen wie der Sportwettenwerbung denkbar. Demnach kann es wohl prinzipiell entsprechende Fälle in Verbindung mit Emotionserkennung geben, die unter Art 5 Abs 1 lit b AI Act subsumiert werden könnten. Allerdings müssten gewisse Spezifika im Sinne der obigen Ausführungen gegeben sein.

In gewissen Fällen könnte es auch einen Zusammenhang zwischen Emotionserkennung und nach Art 5 Abs 1 lit a AI Act verbotenen Systemen geben.

Ansonsten würden wohl prinzipiell in allen drei Use Cases in der Regel Hochrisiko-Systeme gem Art 6 Abs 2 AI Act vorliegen, aufgrund der pauschalen Listung von Systemen, „die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen“, in Anhang III Ziffer 1 lit c AI Act. Dabei ist zwar grundsätzlich die Ausnahmeregelung in Art 6 Abs 3 AI Act zu berücksichtigen. Im Hinblick auf Emotionserkennung im Marketing generell und die genannten Use Cases im Besonderen erscheint allerdings schon fraglich, inwieweit ein entsprechendes KI-System „kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst“.[167] Denn insbesondere in Bezug auf Use Case 4.1 könnten sich Auswirkungen auf die psychische Gesundheit insbesondere von spielsüchtigen Personen ergeben und es sind dabei auch Auswirkungen auf die finanzielle Gesundheit und damit auch die private Lebensführung denkbar. Letzteres könnte unter Umständen auch etwa im Zusammenhang mit Use Case 4.2 vorliegen. Zumindest im Fall des Use Case 4.2 wäre allerdings durchaus auch zu hinterfragen, ob dies bereits ein entsprechend erhebliches Risiko birgt. Zudem könnten die entsprechenden Grundrechte auf Daten- und Privatsphärenschutz (Art 7 und 8 GRC) betroffen sein, insbesondere im Hinblick auf die Verarbeitung potenziell sensibler Daten oder entsprechender Ableitungen.

Eventuell könnte aber zumindest hinsichtlich Use Case 4.3 in Zusammenhang mit der Anpassung bzw Verbesserung von **abgeschlossenen** Dienstleistungen die Bedingung des Art 6 Abs 3 lit b AI Act erfüllt sein, sofern das System nämlich lediglich dazu bestimmt wäre, „das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern“. Dies wäre im ersten Unterfall des Use Case 4.3 (4.3.a) hingegen naturgemäß anders, da hierbei entsprechende Angebote gegebenenfalls schon im Vorhinein angepasst/verbessert würden, wobei noch überhaupt keine menschliche Tätigkeit vorliegen muss. Je nach der Reaktion auf die Emotionsableitung im zweiten Unterfall von Use Case 4.3 (4.3.b), wäre auch hierbei die Heranziehung der Ausnahme eher fraglich, wenn etwa auf eine etwaige Unzufriedenheit wiederum direkt mit einem angepassten Angebot (zB besseren Bankkonditionen) für die betroffene Person reagiert werden würde. Immerhin würde auch dabei schließlich noch nicht unbedingt eine abgeschlossene menschliche Tätigkeit vorliegen.

Somit stellen wohl alle drei Use Cases prinzipiell Hochrisiko-KI-Systeme gem Art 6 Abs 2 AI Act dar, soweit insbesondere bzgl des Use Case 4.3 nicht eine Ausnahme gem Art 6 Abs 3 lit b AI Act in Anspruch genommen werden kann. Manche Konstellationen könnten wiederum sogar verbotene Praktiken gem Art 5 AI Act darstellen.

[167] Siehe insgesamt insbesondere Art 6 Abs 3 AI Act; siehe im Detail Kapitel 5.2.2.

## 5.4 Relevante Bestimmungen der Datenschutz-Grundverordnung (DSGVO)

### 5.4.1 Artikel 22 DSGVO

**Artikel 22 DSGVO**

(1) Die betroffene Person hat das **Recht**, **nicht** einer ausschließlich auf einer **automatisierten Verarbeitung** — einschließlich Profiling — beruhenden **Entscheidung unterworfen zu werden**, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 **gilt nicht**, wenn die **Entscheidung**

a) für den **Abschluss oder die Erfüllung eines Vertrags** zwischen der betroffenen Person und dem Verantwortlichen **erforderlich** ist,
b) aufgrund von **Rechtsvorschriften der Union** oder der **Mitgliedstaaten**, denen der Verantwortliche **unterliegt**, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit **ausdrücklicher Einwilligung** der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen **trifft** der **Verantwortliche** angemessene **Maßnahmen**, um die **Rechte** und **Freiheiten** sowie die **berechtigten Interessen** der betroffenen Person **zu wahren**, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) **Entscheidungen** nach **Absatz 2** dürfen **nicht auf besonderen Kategorien personenbezogener Daten** nach Artikel 9 Absatz 1 **beruhen**, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Wie in Abschnitt 5.1 erläutert, findet sich bereits in der DSGVO mit Art 22 eine Bestimmung zu automatisierten Entscheidungen, der wiederum ein entsprechendes Auskunftsrecht gegenübersteht.

#### 5.4.1.1 Allgemeines

Bei Verarbeitungstätigkeiten nach Art 22 DSGVO handelt es sich um gesteigerte Formen der automatisierten Verarbeitungen, nämlich um Entscheidungen, die ausschließlich auf automatisierten Verarbeitungen beruhen und ausschließlich maschinell – also ohne inhaltliches Eingreifen von Menschen – erfolgen. Damit verfolgt diese Norm – sowie ihre Vorgängerbestimmung Art 15 EG-DSRL – den Ansatz, Menschen vor Maschinenentscheidungen zu schützen, da die Vorgaben von Algorithmen bei Entscheidungen massive Beeinträchtigungen für Betroffene verursachen können.[168] Neben automatisierten Entscheidungen hat der Gesetzgeber auch das Profiling zum Anwendungsfall des Art 22 DSGVO erklärt.[169] Unter Profiling versteht man gemäß Art 4 Z 4 DSGVO „[...] jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass die personenbezogenen Daten verwendet werden, um bestimmte Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.“ Damit thematisiert der Gesetzgeber die Gefahren, die von der Erstellung von Persönlichkeitsprofilen auf Basis personenbezogener Daten und die damit verknüpfte Prognose von zukünftigem Verhalten für die Persönlichkeitsrechte, die Autonomie sowie die Menschenwürde betroffener Personen ausgehen.[170] Außerdem bringt dies zum Ausdruck, dass relativ viele Datenverarbeitungen der Definition von Profiling gem Art 4 Z 4 DSGVO entsprechen und damit der Anwendungsbereich der DSGVO schnell eröffnet ist. Um jedoch auch von Art 22 DSGVO erfasst zu sein, muss das Profiling als „Vorfeldschritt“ zu einer automatisierten Entscheidung führen, die rechtliche Wirkung entfaltet oder Betroffene ähnlich erheblich beeinträchtigt.[171]

**Beispiel**

So kann es sich bei Use Case 2 um einen Fall des Profilings handeln, wenn individuelle Kund:innenprofile auf Basis bestimmter Verhaltensmerkmale erstellt werden, um abwanderungsgefährdete Kund:innen zu identifizieren und entsprechende Maßnahmen einzuleiten. Die Identifikation kann beispielsweise mittels algorithmischer Auswertung von in Social-Media-Beiträgen ausgedrückten Stimmungslagen erfolgen (sog „Sentiment-Analysen“), welche in die Kategorien positiv, negativ oder neutral eingeteilt werden. Anschließend werden die abwanderungsgefährdeten Kund:innen anhand übereinstimmender Merkmale durch den Algorithmus identifiziert. Auf Basis solchermaßen erstellter Profile könnten

[168] Vgl *Weichert* in *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG. Kompaktkommentar³ (2024) Art 22 DSGVO Rz 2 ff.
[169] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 7.
[170] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 9 ff.
[171] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 7.

Unternehmen dann gezielte Maßnahmen setzen, um der Gefahr einer Kundenabwanderung im Vorfeld zu begegnen.[172]

Auch wenn Art 22 Abs 1 DSGVO besagt, dass die betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, bedeutet der Begriff „Recht" nach Ansicht der Artikel-29-Datenschutzgruppe[173] sowie nach Teilen der Lehre[174] nicht, dass Art 22 Abs 1 DSGVO nur dann gelten soll, wenn die betroffene Person von diesem Recht aktiv Gebrauch macht. Art 22 Abs 1 DSGVO verbietet vielmehr generell ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungsfindungen.[175] Dieses Verbot besteht also unabhängig davon, ob die betroffene Person bezüglich der Verarbeitung ihrer personenbezogenen Daten tätig wird.[176] Damit soll dem Umstand Rechnung getragen werden, „dass automatisierte Entscheidungen für die Betroffenen ein besonderes Risiko im Hinblick auf **Transparenz und Beeinflussung** darstellen, so dass die Nutzung des Datenauswertungsvorgangs als besonders sensitiv angesehen wird."[177]

Zu bloßer Entscheidungsunterstützung sind solche Verarbeitungstätigkeiten zulässig, jedoch wirft dies die Frage auf, welche Form der Mitwirkung natürlicher Personen erforderlich ist, damit es sich nicht um eine ausschließlich auf einer automatisierten Entscheidungsfindung beruhenden Entscheidung handelt. Es wird grundsätzlich davon ausgegangen, dass Art 22 DSGVO auf Computerentscheidungen abstellt, die ohne menschliche Einflussnahme getroffen werden, womit Systeme, die eine Entscheidung lediglich vorbereiten, nicht von dessen Anwendungsbereich erfasst sind.[178] Erfolgt eine manuelle Prüfung eines automatisierten Ergebnisses vor einer Entscheidung, die anschließend von einer Person in Abwägung anderer, nicht in das automatisierte Ergebnis eingeflossenen Aspekte bestätigt wird, ist Art 22 DSGVO nicht anwendbar.[179]

In diesem Zusammenhang stellt sich die Frage nach der **„Maßgeblichkeit"** der Entscheidungsbeeinflussung durch den Algorithmus bzw das KI-basierte System, da davon auszugehen ist, dass der Anwendungsbereich von Art 22 DSGVO eröffnet ist, sofern die Entscheidung „maßgeblich" von der Maschine beeinflusst wurde.[180] In seinem bekannten

[172] Vgl *Gausling*, Künstliche Intelligenz im digitalen Marketing, ZD 2019, 335 (338).
[173] Die Artikel-29-Datenschutzgruppe (A29WP) war ein unabhängiges Beratungsgremium der Europäischen Union in Datenschutzfragen und wurde 2018 vom Europäischen Datenschutzausschuss (EDSA) abgelöst, der die einheitliche Anwendung der DSGVO sicherstellen soll. Einige der von der A29WP ausgearbeiteten Leitlinien hat der EDSA bestätigt.
[174] Vgl etwa *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 16.
[175] Vgl EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 52.
[176] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 17/DE WP251rev.01 (2018) 21, https://ec.europa.eu/newsroom/article29/items/612053 .
[177] *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 16.
[178] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 25.
[179] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 25a.
[180] Vgl hier etwa das Erkenntnis des VwGH 21. 12. 2023, Ro 2021/04/0010-11 in Anlehnung an das SCHUFA-Urteil des EuGH (7. 12. 2023, C-634/21, *SCHUFA Holding [Scoring]*, ECLI:EU:C:2023:957) zur Frage, ob es sich beim Arbeitsmarktchancen Assistenzsystem "AMAS" des Österreichischen Arbeitsmarktservice um ein Tool zur

„SCHUFA-Urteil“ (EuGH Rs C-634/21 vom 7. Dezember 2023) hat der EuGH klargestellt, dass bereits die automatisierte Errechnung eines „Creditscores“ durch die Kreditauskunftei „SCHUFA“ in den Anwendungsbereich von Art 22 DSGVO fällt, sofern die anschließende Entscheidung über eine Kreditgewährung maßgeblich auf diesem Scorewert beruht.[181] Die Entscheidung stellt somit auf die in Art 22 DSGVO vorgenommene Differenzierung zwischen „vollautomatisierten“ und „teilautomatisierten“ Entscheidungen ab, wobei erstere auf jeden Fall von Art 22 DSGVO gedeckt sind, während es bei letzteren auf den Grad der Konkretisierung des Entscheidungsvorschlags ankommt, auf dessen Basis eine menschliche Entscheidung getroffen wird.[182] So können sog Vorschlagssysteme, die den menschlichen Entscheidungsträger:innen bereits einen konkreten Entscheidungsausgang nahelegen in den Anwendungsbereich von Art 22 DSGVO fallen (eben die hier angeführte Errechnung eines „Creditscores“ zur Einstufung der Kreditwürdigkeit), während beispielsweise KI-basierte Systeme, die Informationen aufbereiten, analysieren oder visualisieren und somit lediglich unterstützende Aufgaben ausführen (beispielsweise das Sammeln von allgemeinen Hintergrundinformationen durch das bekannte Sprachmodell ChatGPT), nicht davon umfasst sind.[183]

Ein wesentlicher Indikator für Maßgeblichkeit ist darüber hinaus in Bezug auf einen KI-basierten Entscheidungsvorschlag das als sog „Automation Bias“ bekannte sozio-technische Phänomen des besonderen Vertrauens in die Ausgaben von KI-Systemen, das durch Intransparenz des Systems und einen potenziellen Rechtfertigungsdruck bei Abweichungen von dem KI-basierten Entscheidungsvorschlag durch menschliche Entscheidungsträger:innen begünstigt wird (nähere Informationen finden sich in Kapitel 6).[184]

Festzuhalten ist, dass die menschliche Beteiligung nicht nur pro forma erfolgen darf, um den Anwendungsbereich von Art 22 DSGVO auszuschließen, und Verantwortliche somit dafür sorgen müssen, dass es sich nicht nur um eine symbolische Geste handelt, sondern Entscheidungen einer echten Aufsicht unterliegen und die Entscheidungen von einer Person getroffen werden sollten, die zur Änderung derselben befugt und befähigt ist.[185]

#### 5.4.1.2 „Entscheidung“

Ganz grundsätzlich fordert Art 22 DSGVO, dass eine Entscheidung vorliegen muss. Das Konzept der Entscheidung ist in der DSGVO nicht eindeutig definiert, der EuGH tendiert jedoch in seiner Spruchpraxis dazu, den Begriff „Entscheidung“ weit auszulegen.[186] Weiters scheint

automatisierten Entscheidungsfindung nach Art 22 DSGVO handelt. Das Verfahren wurde wieder an das BVwG mit der Begründung zurückverwiesen, dass dieses noch zu klären habe, ob die Entscheidung über die Arbeitsmarktchancen einer Person “maßgeblich“ von dem System beeinflusst werde.

[181] Vgl dazu auch *Paal/Hüger,* MMR 2024, 540 (541).

[182] Vgl *Paal/Hüger,* MMR 2024, 540 (541).

[183] Vgl *Paal/Hüger,* MMR 2024, 540 (541 f).

[184] Vgl *Paal/Hüger,* MMR 2024, 540 (542).

[185] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 22; *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 25.

[186] Vgl *Metikos/Ausloos*, Law, Innovation, and Technology 2025, iE, und EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 45.

sich der Wortlaut von Art 22 DSGVO auf einen einzelnen „Entscheidungsmoment“ zu beziehen und dabei auszublenden, dass in der Praxis oftmals mehrere Handlungen oder Aktionen Einfluss auf die letztendliche Entscheidungsfindung haben.[187] Folgt man einer derartigen Interpretation, so könnte dies einer Umgehung der Rechtsfolgen von Art 22 DSGVO durch ein Ausklammern von „Vor-Entscheidungen“[188] Tür und Tor öffnen und eine Rechtsschutzlücke hinterlassen, weshalb der EuGH davon ausgeht, dass auch maßgebliche Vor-Entscheidungen in den Anwendungsbereich von Art 22 DSGVO fallen, sofern die Haupt-Entscheidung stark auf diesen beruht.[189] Dass der Begriff „Entscheidung“ weit auszulegen ist, wird auch in der Literatur unterstrichen, wo bspw *Weichert* davon ausgeht, dass anstatt von einer Entscheidung auch von einer Maßnahme gesprochen werden kann.[190]

**Beispiel**

Dass der Begriff „Entscheidung“ weit auszulegen ist und auch maßgebliche Vor-Entscheidungen umfassen kann, kommt in Use Case 3 zur Bonitäts- und Kreditwürdigkeitsprüfung zum Ausdruck. Hier geht der EuGH davon aus, dass bereits die Ermittlung eines Score-Wertes als solche als Entscheidung einzustufen ist, die im Sinne von Art 22 Abs 1 DSGVO gegenüber einer betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, sofern dieser Score maßgeblichen Einfluss auf die Entscheidung hat.[191]

#### 5.4.1.3 „Rechtliche Wirkung“

Zudem müssen die automatisierten Entscheidungsfindungen nach Art 22 Abs 1 DSGVO rechtliche Wirkungen für Betroffene mit sich bringen oder Betroffene in ähnlicher Weise erheblich beeinträchtigen. Die Entscheidung muss laut Artikel-29-Datenschutzgruppe die Rechte einer Person betreffen. Dies könnte etwa die Vereinigungsfreiheit, das Wahlrecht oder das Recht, rechtliche Schritte einzuleiten, den rechtlichen Status einer Person oder die Betroffenheit von deren Rechten aus einem Vertrag betreffen.

[187] Vgl *Metikos/Ausloos*, Law, Innovation, and Technology 2025, iE.
[188] Vgl *Binns/Veale*, Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR, International Data Privacy Law 2021, 319.
[189] Vgl *Metikos/Ausloos*, Law, Innovation, and Technology 2025, iE, und EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 61f.
[190] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 25. Einer ähnlichen Argumentation folgend: *Haidinger* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 22 DSGVO Rz 18 (Stand 1. 12. 2022, rdb.at) unter Berufung auf ErwGr 71 Satz 1.
[191] EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 50.

**Beispiel**

Als konkrete Beispiele werden etwa die Auflösung eines Vertrags, der Anspruch auf bzw die Verweigerung einer bestimmten gesetzlichen Sozialleistung wie zB Kindergeld oder Wohngeld oder eine Einreiseverweigerung in ein Land oder die Ablehnung der Einbürgerung genannt. Praktische Anwendungsfälle für Entscheidungen, die rechtliche Wirkung entfalten, sind weiters das Profiling zur Online-Gewährung von Krediten oder die Durchführung von Online-Einstellungsverfahren (ErwGr 71 DSGVO).[192]

Dem Wortlaut nach würde das Erfordernis der rechtlichen Wirkung auch positive Wirkungen umfassen (siehe im Gegensatz dazu die Parallelvorschrift des Art 11 Abs 1 DSRL-PJ, die von nachteiligen Rechtsfolgen spricht). Teile der Lehre gehen davon aus, dass es keine Rolle spielt, ob die rechtliche Wirkung für Betroffene positiv oder negativ ist, da eine Nachteilswirkung explizit nicht gefordert wird.[193] Das Ziel der Norm spricht hingegen dafür, dass hier nur negative rechtliche Auswirkungen umfasst sein sollen, die rechtliche Wirkung also erheblich beeinträchtigen muss.[194] Es muss jedoch in Betracht gezogen werden, dass einer „negativen" Wirkung gewissermaßen auch immer eine subjektive Komponente innewohnt, die aus Betroffenensicht nicht immer leicht darzulegen ist.[195] Eine Entscheidung kann zwar objektiv „positiv" sein, allerdings hätte diese aus Betroffenensicht noch weitaus positiver ausfallen können, weshalb sie aus Perspektive der betroffenen Person in Summe als „negativ" empfunden wird (bspw die automatisierte Einstufung in ein bestimmtes Gehaltsschema beim Eingehen eines neuen Beschäftigungsverhältnisses). Außerdem – sofern eine *ex ante*-Betrachtung vor einer konkreten Entscheidung erfolgt – besteht stets die Möglichkeit einer Beeinträchtigung durch eine konkrete Entscheidung, da mehrere Ausgänge der Entscheidung möglich sind und sich jeder potenzielle Ausgang der Entscheidung auf die betroffene Person im Vergleich zu alternativen Optionen negativ auswirken könnte. Weiters ist es nicht immer der Fall, dass eine Entscheidung nur eine bestimmte rechtliche Wirkung entfaltet und somit klar als ausschließlich „positiv" oder „negativ" bewertet werden kann. So könnte einem bestimmten Antrag (bspw auf eine Baubewilligung) nur teilweise stattgegeben werden, womit die Entscheidung sowohl positive Aspekte iSe positiven Erledigung als auch negative Aspekte iSe Ablehnung gewisser Teile des Antrags umfasst.

Zusammengefasst lässt sich somit die Positivität oder Negativität einer rechtlichen Wirkung nicht objektiv bewerten bzw diese nicht als ausschließlich „negativ" oder ausschließlich „positiv" bezeichnen. Außerdem gilt es zu bedenken, dass es sich bei Art 22 DSGVO - im Unterschied zu Art 86 AI Act - um eine ausdrückliche Verbotsnorm handelt, weshalb hier

[192] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 23.
[193] Vgl etwa *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 27.
[194] *Herbst* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG[8] (2024) Art 15 DSGVO Rz 13 ff; *Kamlah* in *Plath* DSGVO/BDSG/TTDSG[4] (2023) Art 22 DSGVO Rz 17.
[195] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 27.

besonders auf die Betroffenensicht einzugehen ist. Und da dieser Meinungsstreit nicht abschließend geklärt ist, ist an dieser Stelle zu empfehlen, das Erfordernis der rechtlichen Wirkung weit auszulegen und daher jede Auswirkung, unabhängig von einer versuchten Kategorisierung als positiv oder negativ, zu erfassen.

#### 5.4.1.4 Der Ausdruck „sie in ähnlicher Weise erheblich beeinträchtigt“

Die Grenze, ab wann Betroffene in ähnlicher Weise erheblich beeinträchtigt sind, ist laut der Artikel-29-Datenschutzgruppe ähnlich zu sehen wie die Grenze, ab der eine Entscheidung rechtliche Wirkung entfaltet. Die Wirkung muss dabei umfassend sein und die Möglichkeit bestehen, dass die Entscheidung:

- die Umstände, das Verhalten oder die Entscheidungen der betroffenen Personen erheblich beeinträchtigt;
- die betroffene Person über einen längeren Zeitraum oder dauerhaft beeinträchtigt oder
- im schlimmsten Fall zum Ausschluss oder zur Diskriminierung von Personen führt.

in diese Kategorie könnten folgende Entscheidungen fallen:

- Entscheidungen, die sich auf die finanzielle Lage einer Person auswirken, beispielsweise ihre Kreditwürdigkeit;
- Entscheidungen, die den Zugang zu Gesundheitsdienstleistungen betreffen;
- Entscheidungen, die den Zugang zu Arbeitsplätzen verwehren oder Personen ernsthaft benachteiligen;
- Entscheidungen, die sich auf den Zugang zu Bildung auswirken, beispielsweise Hochschulzulassungen

## Erwägungsgrund 71

Die **betroffene Person** sollte das **Recht** haben, **keiner Entscheidung** – was eine Maßnahme einschließen kann – zur Bewertung von sie betreffenden persönlichen Aspekten **unterworfen zu werden**, die **ausschließlich auf** einer **automatisierten Verarbeitung beruht** und die rechtliche Wirkung für die betroffene Person entfaltet **oder sie in ähnlicher Weise erheblich beeinträchtigt**, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen.

Zu einer derartigen Verarbeitung zählt auch das „**Profiling**", das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. [...]

Erwägungsgrund 71 DSGVO erwähnt folgende typische Beispiele: „automatische Ablehnung eines Online-Kreditantrags" oder „Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen". Von den eingangs präsentierten Use Cases können an dieser Stelle gewisse Formen der Schaltung von Online-Werbung auf Basis von Emotionserkennung genannt werden, welche eine Form des Profiling darstellen können und somit vom Anwendungsbereich des Art 22 DSGVO erfasst wären.[196] Eine erhebliche Beeinträchtigung durch Werbung liegt vor, wenn ein „Tracking" bzw eine „Verfolgung" von Personen über mehrere Webseiten oder Dienste erfolgt und auf die Erwartungen und Bedürfnisse dieser Personen abgestimmte Werbung geschaltet wird.[197] Dies trifft wohl auf die meisten Werbeschaltungen zu, sofern diese über mehrere Geräte oder Internetseiten geschaltet werden oder in Form von „Retargeting" zu einer unzumutbaren Belästigung der betroffenen Person führen.[198] Laut der Artikel-29-Datenschutzgruppe wird jedoch im Bereich der Online-Werbung die Entscheidung, auf Profiling beruhende gezielte Werbung zu präsentieren, Personen nicht in ähnlicher Weise erheblich beeinträchtigen, wenn Werbung für einen Online-Shop eines Mainstream-Modehändlers angezeigt wird, die auf einem einfachen demografischen Profil beruht. Erfasst sind hingegen diskriminierende Werbungen, personalisierte Preisangebote oder Werbeanzeigen, die gezielt Schwachstellen von Betroffenen ansprechen und ausnutzen,[199] wie beispielsweise an spielsüchtige Personen gerichtete Werbeschaltungen für Sportwetten. Differenziert wird die Situation somit bei einem eingreifenden Charakter des Profiling-

[196] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 31.
[197] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 31.
[198] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 31
[199] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 31.

Prozesses oder wenn jemand, der sich bekanntermaßen oder wahrscheinlich in finanziellen Schwierigkeiten befindet und regelmäßig gezielte Werbung für hochverzinsliche Darlehen erhält, diese Angebote unterschreibt und dadurch möglicherweise weitere Schulden aufnimmt, betrachtet.[200] Erwähnt wird, dass auch das Handeln anderer Personen, als derjenigen, auf die sich die automatisierte Entscheidung bezieht, ähnliche erhebliche Beeinträchtigungen auslösen kann, wie etwa die Festlegung von Kreditkartenlimits nicht auf Basis des eigenen Rückzahlungsverhaltens sondern des Verhaltens, das sich auf Basis der Analyse von anderen Kund:innen ergeben hat.[201] Ein anderer Fall betrifft die automatisierte Entscheidung über einen Energieliefervertrag, dessen Stornierung aufgrund mangelnder Bonität vorgenommen wird, ohne dass negative Zahlungserfahrungsdaten der betroffenen Person vorliegen.[202]

#### 5.4.1.5 Ausnahmen vom Verbot der automatisierten Entscheidungsfindung

In Art 22 Abs 2 DSGVO werden jedoch auch Ausnahmen vom grundsätzlichen Verarbeitungsverbot abschließend festgelegt. Das automatisierte Verarbeitungsverbot gilt somit nicht, wenn die automatisierte Entscheidungsfindung:

a) für die Erfüllung oder den Abschluss eines Vertrags erforderlich ist;

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Betrifft die Entscheidung in Artikel 9 Absatz 1 definierte besondere Datenkategorien, muss der Verantwortliche zudem die Einhaltung der Bedingungen von Artikel 22 Absatz 4 sicherstellen, beispielsweise das Treffen von angemessenen Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person.

Angesichts der zunehmenden Digitalisierung unserer Rechtsbeziehungen nehmen automatisierte Entscheidungsprozesse in allen Lebensbereichen zu, so auch in Vertragsverhältnissen.[203] Die Artikel-29-Datenschutzgruppe führt folgendes Beispiel für die Vertragserfüllung nach Art 22 Abs 2 lit a DSGVO an:

**Beispiel**

Ein Unternehmen veröffentlicht eine Stellenanzeige. Da das Unternehmen ein

[200] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 23 f.
[201] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 23 f.
[202] Vgl BVwG 23. 4. 2024, W292 22488672-1/5E.
[203] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 43.

beliebter Arbeitgeber ist, gehen zehntausende Bewerbungen ein. Aufgrund der außergewöhnlich hohen Anzahl an Bewerbungen sieht es das Unternehmen als praktisch unmöglich an, passende Bewerber zu ermitteln, ohne nicht infrage kommende Bewerbungen mithilfe vollständig automatisierter Verfahren auszusortieren. In diesem Fall kann eine automatisierte Entscheidungsfindung erforderlich sein, um eine kurze Liste möglicher Bewerber zu erstellen, mit der Absicht, mit einer betroffenen Person einen Vertrag zu schließen.[204]

In Bezug auf den Erlaubnistatbestand der Rechtsvorschriften gem Art 22 Abs 2 lit b DSGVO spricht man von einer Öffnungsklausel, wodurch eine Konkretisierungsbefugnis im Unions- oder im nationalen Recht eingeräumt wird.[205] Derartige Rechtsvorschriften müssen demokratisch legitimiert sein und dienen häufig bestimmten hoheitlichen Zielsetzungen, wie etwa der Bekämpfung von Betrug oder nationalen Sicherheitszwecken.[206]

Erlaubt ist eine automatisierte Entscheidung außerdem auf Basis einer ausdrücklichen Einwilligung der betroffenen Person, deren Wirksamkeit an hohe Voraussetzungen in Bezug auf die Informiertheit, Bestimmtheit der Erklärung und die Freiwilligkeit geknüpft ist.[207] Mindestvoraussetzung ist, dass zumindest die Logik der Verarbeitung, der Daten-Input, der Zweck der Verarbeitung bzw der Entscheidung sowie die beteiligten Stellen offengelegt werden.[208]

Von besonderer Bedeutung sind zudem die Transparenzpflichten, die in der DSGVO für automatisierte Entscheidungsfindungen vorgesehen sind, wie etwa das Recht auf Information bzw Auskunft (gem den Art 13, 14 und 15 hier insbesondere der Erhalt aussagekräftiger Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen für die betroffene Person) und Garantien wie das Recht auf Erwirkung des Eingreifens einer Person oder das Recht auf Anfechtung der Entscheidung (siehe Art 22 Abs 3 DSGVO).

[204] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 25.
[205] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 37.
[206] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 37 f.
[207] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 46.
[208] Vgl *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO Rz 47.

## Beispiel

**Praktische Veranschaulichung des Art 22 DSGVO anhand des Fallbeispiels der Bonitäts- und Kreditwürdigkeitsprüfung:**

In Bezug auf die praktischen Implikationen von Art 22 DSGVO hat kaum ein Fall so viel Interesse geweckt wie jener der Bonitätsbewertung und Kreditwürdigkeitsprüfung, insbesondere durch das bereits mehrfach zitierte „SCHUFA-Urteil“, worin der EuGH den Begriff der „automatisierten Entscheidung im Einzelfall“ weit auslegt.[209]

Eine solche liegt vor, wenn ein auf personenbezogene Daten gestützter Wahrscheinlichkeitswert in Bezug auf die Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet. In diesem Fall ist bereits die Ermittlung dieses Wertes als solche als Entscheidung einzustufen, die im Sinne von Art 22 Abs 1 DSGVO gegenüber einer betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[210]

Ein zentraler Punkt des Urteils ist, dass bereits die Erstellung des Scores als eine automatisierte Entscheidung im Sinne des Art 22 DSGVO angesehen werden kann, wenn dieser Score maßgeblichen Einfluss auf die Entscheidung eines Dritten (zB einer Bank) hat. Dies ist ein wichtiger Unterschied zu Art 86 AI Act, der eine niedrigere Schwelle ansetzt: Hier reicht es aus, wenn der Einfluss von Relevanz ist, ohne dass er „maßgeblich“ sein muss (Näheres dazu findet sich in Abschnitt 5.5).

Eine offene Frage, die der EuGH nicht abschließend geklärt hat, ist, ob auch reine statistische Algorithmen bereits unter den Begriff der automatisierten Entscheidung nach Art 22 DSGVO bzw den KI-Begriff fallen. Art 3 AI Act definiert KI-Systeme als solche, die mindestens teilweise autonom agieren. Dies bedeutet, dass das System nicht ausschließlich auf von Menschen vorgegebenen statischen, deterministischen Regeln basiert, sondern seine Entscheidungslogik über die reine Datenverarbeitung hinausgeht, indem es Lernen, Schlussfolgerungen oder Modellierung ermöglicht.[211]

Autonomie wird hier als Abgrenzung zu klassischen „Wenn-Dann-Systemen“ verstanden, deren Output vollständig durch vom Menschen vorgegebene Regeln bestimmt wird. Bei KI-Systemen hingegen wird die Entscheidungslogik indirekt beispielsweise durch maschinelles Lernen geprägt, sodass der Output nicht vollständig vom Menschen vorhersehbar oder vorgegeben ist. Dies könnte als Lücke im AI Act angesehen werden, da komplexe deterministische Systeme, die von KI erstellt wurden, ähnliche Ergebnisse wie autonome KI-Systeme liefern können und Menschen ihre Funktion bzw Entscheidungslogik nicht mehr verstehen, aber nicht unter die

[209] EuGH 7. 12. 2023, C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957.
[210] EuGH 7. 12. 2023, C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957, Rz 50.
[211] Vgl ErwGr 12 AI Act.

Regulierung fallen.[212]

Eine Klarstellung hat jedenfalls entlang der durch den AI Act vorgegebenen Definitionen zu erfolgen. So kam es im Vorfeld der Publikation der Leitlinien zum Begriff des KI-Systems zu internen Auseinandersetzungen, ob lineare/logistische Regression, eine simple Machine-Learning-Technik, die im Finanzbereich von großer Relevanz ist, unter den Begriff und damit in den Anwendungsbereich des AI Act fallen sollte.[213]

Die veröffentlichten Leitlinien sehen vor, dass solche gebräuchlichen Machine-Learning-Ansätze nicht unter den Begriff des KI-Systems fallen.[214]

[212] *Rosenthal*, Der EU AI Act – Verordnung über künstliche Intelligenz, Jusletter 5. 8. 2024, 1 (7).
[213] *Bertuzzi*, Financial sector sees last-minute disagreements over EU's definition of AI system, https://www.mlex.com/mlex/articles/2293541/financial-sector-sees-last-minute-disagreements-over-eu-s-definition-of-ai-system (Stand: 5.2.2025).
[214] Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final 8.

### 5.4.2 Artikel 15 Abs 1 lit h DSGVO

**Artikel 15 DSGVO**

1. Die betroffene Person hat das **Recht**, von dem Verantwortlichen eine **Bestätigung** darüber zu **verlangen**, **ob** sie betreffende **personenbezogene Daten verarbeitet** werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf folgende Informationen:

a. die **Verarbeitungszwecke**;

b. die **Kategorien** personenbezogener Daten, die verarbeitet werden;

c. die **Empfänger oder Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d. falls möglich die **geplante Dauer**, für die die personenbezogenen Daten **gespeichert** werden, oder, falls dies nicht möglich ist, die **Kriterien** für die Festlegung dieser Dauer;

e. das Bestehen eines **Rechts auf Berichtigung oder Löschung** der sie betreffenden personenbezogenen Daten oder auf **Einschränkung der Verarbeitung** durch den Verantwortlichen oder eines **Widerspruchsrechts** gegen diese Verarbeitung;

f. das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde;

g. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, **alle verfügbaren Informationen über die Herkunft der Daten**;

h. das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich Profiling gem Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – **aussagekräftige Informationen über die involvierte Logik** sowie die **Tragweite** und die **angestrebten Auswirkungen** einer derartigen Verarbeitung für die betroffene Person.

#### 5.4.2.1 Einleitung

Nach Art 15 DSGVO haben Betroffene das Recht, vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Falls dies der Fall ist, so hat die betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten und auf eine Reihe von Informationen. Als Spezialfall listet Art 15

Abs 1 lit h DSGVO in Bezug auf die automatisierte Entscheidungsfindung drei Informationselemente, über die Auskunft gegeben werden muss: 1. “das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – [2.] aussagekräftige Informationen über die involvierte Logik sowie [3.] die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.“

#### 5.4.2.2 Involvierte Logik

Im Zentrum der folgenden Ausführungen steht dabei das Element der „involvierten Logik“, das in Literatur und Judikatur für zahlreiche Diskussionen gesorgt hat. In der Literatur werden die notwendigen Informationselemente häufig wiederum, ohne sie zu konkretisieren, durch andere Begriffe wie „Logik“, „logischer Aufbau“, „Grundannahmen der Algorithmus Logik“, „Entscheidungslogik“ oder „Methoden und Kriterien der Datenverarbeitung“ umschrieben.[215]

Umstritten ist dabei, ob neben abstrakt gehaltenen Informationen über die Wirkungsweise und Relevanz des Entscheidungssystems auch eine Verpflichtung zur einzelfallbezogenen Begründung konkreter Verarbeitungsergebnisse besteht. Dies wird von der überwiegenden Lehre primär mit Verweis auf den Gleichklang mit Art 13 und 14 DSGVO, die chronologisch vor der Entscheidungsfindung ansetzen, verneint.[216]

Für die Identität der Informationen scheinen auch die Leitlinien der A29WP, die vom EDBP übernommen wurden, zu sprechen: „Der Verantwortliche sollte der betroffenen Person diese Informationen in Übereinstimmung mit seinen Pflichten nach Artikel 13 bereits zur Verfügung gestellt haben.“[217] Weiters: „Der Verantwortliche sollte der betroffenen Person allgemeine Informationen übermitteln (vor allem zu bei der Entscheidungsfindung berücksichtigten Faktoren und deren „Gewichtung“ auf aggregierter Ebene), die auch für die Anfechtung der Entscheidung seitens der betroffenen Person nützlich sind.“[218]

Dem widersprechend führen aktuellere Leitlinien des EDPB aus, dass „wenn möglich, [...] die Informationen gem Artikel 15 Absatz 1 Buchstabe h die genauen Gründe enthalten [müssen], die zu bestimmten Entscheidungen in Bezug auf die betroffene Person, die um Auskunft ersucht, geführt haben.“[219] Diese Aussage wird jedoch durch die Beifügung von „wenn möglich“ relativiert.

Eine andere Ansicht, die für eine einzelfallbezogene Begründung spricht, wird bspw von *Bäcker* vertreten, der argumentiert, dass die Funktion des Auskunftsanspruches sei, eine wirksame Wahrnehmung der Rechte und Freiheiten zu ermöglichen. Ohne eine solche

[215] *Schneeberger*, Machine Learning 167.
[216] Grundlegend *Wachter/Mittelstadt/Floridi*, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law 2017, 76; mwN *Schneeberger*, Machine Learning 171 ff.
[217] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 29.
[218] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 30.
[219] *EDPB*, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht Version 2.1 (2023) 48, https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_de.pdf .

Begründung könnte dem Black-Box-Charakter des Entscheidungsprozesses wenig entgegengesetzt werden.[220]

In diese Richtung argumentiert auch *Franck*, nach dem ohne entsprechendes „Begründungsmaterial“ die Darlegung des eigenen Standpunktes und die Anfechtung der Entscheidung iSv Art 22 Abs 3 DSGVO nicht sinnvoll möglich ist.[221]

Ebenso müssen nach *Mester* über die Methoden und Kriterien sowie die Tragweite und Auswirkungen der Datenverarbeitung hinaus „außerdem die bereits ermittelten Auswertungsergebnisse sowie die darauf beruhenden Entscheidungen mitgeteilt werden.“[222] Ähnlich müssen nach *Däubler* auch „in der Vergangenheit liegende Auswertungen sowie die auf dieser Grundlage getroffenen Entscheidungen“[223] mitgeteilt werden. Auch nach *Dix* ist vor dem Hintergrund des Ziels, den Betroffenen die Ausübung ihrer Rechte zu ermöglichen, die Annahme eines (einzelfallbezogenen) Rechts auf Erläuterung, gestützt auf Art 15 DSGVO, notwendig, um den Informationsasymmetrien Herr zu werden.[224]

Ähnliche Argumentationslinien, die für die Existenz eines Rechtes auf einzelfallbezogene Erklärung sprechen, finden sich bspw bei *Kaminski*,[225] *Malgieri* und *Comandé*,[226] *Hacker* und *Passoth*[227] und *Selbst* und *Powles*.[228]

Nach einem interdisziplinären Bericht, der die involvierte Logik aus einer kombinierten technischen und rechtlichen Perspektive betrachtet, gibt es verschiedene Möglichkeiten, die involvierte Logik entsprechend darzustellen: „We think that the demand for documenting the input data, architectural choices and evaluation methods falls under what was called the ‘structure and sequence of the data processing’ in the legal considerations above. We propose to make the design and development process of the ADM system as well as the underlying rationale transparent. This may require obligations to document the processes of data gathering and preparation including annotation or labelling. Ensuring the highest amount of transparency at the input level is arguably one of the best ways to influence and truly understand what is happening in a model. Likewise, instantiating the demand of showing the ‘logic involved’ by the more concrete requirement of providing local or global explanations of the socio-technical systems can be seen as an operalisation step.“[229]

---

[220] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG. Kommentar[4] (2024) Art 15 DSGVO Rz 27b f.
[221] *Franck* in *Gola/Heckmann*, Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz. Kommentar[3] (2022) Art 15 DSGVO Rz 18.
[222] *Mester* in *Taeger/Gabel*, DSGVO - BDSG - TTDSG[4] (2022) Art 15 DSGVO Rz 12.
[223] *Däubler* in *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG. Kompaktkommentar[3] (2024) Art 15 DSGVO Rz 18.
[224] *Dix* in *Spiecker gen. Döhmann/Papakonstantinou/Hornung/Hert*, General Data Protection Regulation. Article-by-Article Commentary (2023) Art 15 GDPR Rz 19.
[225] *Kaminski*, The Right to Explanation, Explained, Berkeley Technology Law Journal 2019, 189.
[226] *Malgieri/Comandé*, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law 2017, 243.
[227] *Hacker/Passoth*, Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond, in *Holzinger/Goebel/Fong/Moon/Müller/Samek* (Hrsg), xxAI - Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020 July 18, 2020, Vienna, Austria, Revised and Extended Papers (2022) 343 (348 f).
[228] *Selbst/Powles*, Meaningful information and the right to explanation, International Data Privacy Law 2017, 233.
[229] *Asghari et al*, What to explain 18. MwN zu einer solchen interdisziplinären Betrachtung *Bibal/Lognoul/Streel/Frénay*, Legal requirements on explainability in machine learning, AI and Law 2021, 149;

Eine lokale Erklärung bezeichnet dabei im Forschungsbereich explainable AI die Erklärung einer Einzelentscheidung, was auch für komplexere Modelle (zB Künstliche Neuronale Netze) technisch bspw durch Hervorhebung der wichtigsten Merkmale (bspw Pixel in einem Bild) möglich ist. Eine globale Erklärung, die ein Modell unabhängig von einer Einzelentscheidung erläutert, ist technisch komplexer und häufig nur für sog White-Box-Modelle (zB lineare Modelle, Entscheidungsbäume) möglich.[230]

Nach einer Entscheidung der DSB aus dem Jahr 2020 sind „konkret für eine Auskunft gem Art. 15 Abs. 1 lit. h DSGVO die Parameter/Eingangsvariablen einer errechneten Zuordnung, ihr Einfluss auf die errechnete Zuordnung, also im Wesentlichen die Gewichtung der Parameter, die Informationen zum Zustandekommen der Parameter/Eingangsvariablen (bspw. ob der Parameter „Wohnumfeld“ statistisch hochgerechnet wurde), eine Erklärung, weshalb der Betroffene einem bestimmten Bewertungsergebnis zugeordnet wurde und eine Aufzählung der Profilkategorien, die für eine Zuordnung möglich sind, zu beauskunften [...] oder ähnliche dem Informationsgehalt gleichwertige Informationen zu geben, die den Betroffenen in die Lage versetzen, seine Rechte auf Richtigstellung, Löschung und Überprüfung der Rechtmäßigkeit wahrzunehmen.“[231] Die DSB stützte sich dabei auf Ausführungen von *Zavadil*,[232] der selbst Mitarbeiter der DSB ist.

Nach einem Erkenntnis des BVwG[233] hat der Verantwortliche „im Rahmen der Auskunft der betroffenen Person die verwendete Logik derart zu umschreiben, dass diese über die in die Bewertung eingehenden Parameter informiert wird und sie dabei erkennen kann, welche Aspekte ihrer Person oder ihres Verhaltens verwendet werden. Der Algorithmus selbst ist nicht zu beauskunften. Der Begriff der involvierten Logik ist so zu verstehen, dass lediglich das Prinzip darzustellen ist, auf dem eine derartige Berechnung basiert, nicht jedoch die konkrete Berechnungsformel“. Dies deutet wiederum auf eine Erklärung hin, die nicht speziell auf den Einzelfall abstellt, sondern allgemeine Informationen auf aggregierter Ebene bereitstellt (insb die in die Bewertung eingehenden Parameter).

Im SCHUFA-Urteil,[234] in dem der Anwendungsbereich von Art 22 DSGVO konkretisiert wurde, wurde dieser Aspekt nicht spezifiziert. Die SA von GA *Pikamäe* gingen jedoch näher auf die Interpretation der involvierten Logik ein. Nach ihnen umfasst die involvierte Logik nicht „eine etwaige Verpflichtung zur Offenlegung des Algorithmus unter Berücksichtigung seiner Komplexität“. Der Generalanwalt war „der Ansicht, dass die Verpflichtung, ‘aussagekräftige Informationen über die involvierte Logik’ bereitzustellen, dahin zu verstehen ist, dass sie hinreichend detaillierte Erläuterungen zur Methode für die Berechnung des Score-Wertes und zu den Gründen umfasst, die zu einem bestimmten Ergebnis geführt haben. Generell sollte der Verantwortliche der betroffenen Person allgemeine Informationen übermitteln, vor allem

*Brkan/Bonnet*, Legal and Technical Feasibility of the GDPR’s Quest for Explanation of Algorithmic Decisions. Of Black Boxes, White Boxes and Fata Morganas, European Journal of Risk Regulation 2019, 18.

[230] *Schneeberger*, Machine Learning 150 ff.

[231] DSB 8. 9 . 2020, 2020-0.436.002.

[232] *Zavadil*, Das Auskunftsrecht nach Art. 15 Datenschutz-Grundverordnung, Dissertation Universität Wien (2020) 124 f; *Zavadil*, Der besondere Auskunftsanspruch über die involvierte Logik einer Datenverarbeitung, Dako 2020, 55.

[233] BVwG 23. 4. 2024, W292 2248672-1.

[234] EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957.

zu bei der Entscheidungsfindung berücksichtigten Faktoren und deren Gewichtung auf aggregierter Ebene, die auch für die Anfechtung von „Entscheidungen“ im Sinne von Art. 22 Abs. 1 DSGVO seitens der betroffenen Person nützlich sind.“[235]

Dies deutet einerseits auf eine einzelfallbezogene Erklärung hin („die zu einem **bestimmten** Ergebnis geführt haben“). Scheinbar widersprüchlich führen die SA jedoch aus, dass generell „allgemeine Informationen“ zu übermitteln wären „vor allem zu bei der Entscheidungsfindung berücksichtigten Faktoren und deren Gewichtung auf aggregierter Ebene“. Der Hinweis auf die aggregierte Ebene würde wiederum gegen eine einzelfallbezogene Erklärung sprechen.[236] Möglicherweise sind diese allgemeinen Informationen als Basisinformation zu verstehen, die durch konkretere einzelfallbezogene Informationen zu präzisieren sind.

Darauf aufbauend führte GA *de la Tour* in den SA zu *Dun & Bradstreet Austria* zur involvierten Logik aus: „Die Kenntnis dieses Kontexts muss die betroffene Person in die Lage versetzen, das Ergebnis der automatisierten Entscheidung nachzuvollziehen, weil sie die wesentlichen Elemente der Methode und der herangezogenen Kriterien kennt. Im Grunde genommen muss der – naturgemäß technische – Prozess, der zu dieser Entscheidung geführt hat, verständlich gemacht werden. Nur so kann die betroffene Person die ihr durch die DSGVO verliehenen Rechte ausüben [...]. Der Begriff ‘aussagekräftige Informationen über die [bei einer automatisierten Entscheidungsfindung] involvierte Logik’ muss somit funktional verstanden werden. [...] Daher bin ich der Ansicht, dass ‘aussagekräftige Informationen über die [bei einer automatisierten Entscheidungsfindung] involvierte Logik’ es der betroffenen Person ermöglichen müssen, die ihr durch die DSGVO und insbesondere durch Art. 22 dieser Verordnung garantierten Rechte auszuüben. Das setzt erstens voraus, dass die betroffene Person präzise, leicht zugängliche, verständliche sowie in klarer und einfacher Sprache abgefasste Informationen über die für eine solche Entscheidung verwendete Methode und die dafür herangezogenen Kriterien erhalten kann. Zweitens müssen diese Informationen hinreichend vollständig und kontextbezogen sein […]. [...] Daraus schließe ich, dass der Verantwortliche gemäß Art. 15 Abs. 1 Buchst. h DSGVO nicht verpflichtet ist, der betroffenen Person Informationen technischer Art zu übermitteln, die diese nicht verstehen könnte, wie beispielsweise Einzelheiten zu den verwendeten Algorithmen. Dagegen muss er seiner Pflicht nachkommen, der betroffenen Person in jedem Fall sowohl zugängliche als auch hinreichend vollständige Informationen über den Prozess, der zur fraglichen automatisierten Entscheidung geführt hat, sowie über die Gründe für das Ergebnis dieser Entscheidung zur Verfügung zu stellen. So definiert, sollten ‘aussagekräftige Informationen über die [bei einer automatisierten Entscheidungsfindung] involvierte Logik’ u. a. **die verwendete Methode und die berücksichtigten Kriterien sowie deren Gewichtung beschreiben**. Die betroffene Person muss daher nachvollziehen können, welche Informationen bei der automatisierten Entscheidungsfindung verwendet und wie sie berücksichtigt und gewichtet worden sind.“[237]

Auch diese SA stellen wieder stark auf die Methode und die Kriterien der Entscheidung ab.

[235] SA GA *Pikamäe* 7. 3. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:220, Rz 56 ff.
[236] MwN *Schneeberger*, Large Language Models in der Verwaltung, in *Hoffberger-Pippan/Ladeck/Ivankovics* (Hrsg), Digitalisierung und Recht. Jahrbuch 2024 (2024) 223.
[237] SA GA *de la Tour* 12. 9. 2024, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:745, Rz 64 ff (Hervorhebungen durch Autor:innen).

Zudem wird klargestellt, dass der Begriff der aussagekräftigen Informationen funktional zu verstehen ist.[238]

Zu technische Informationen, zB der Algorithmus selbst, müssten, da die Informationen im Sinne des Transparenzgebotes immer verständlich bleiben sollten, nicht preisgegeben werden. Verlangt wird somit auf technischer Ebene primär eine feature-importance-explanation, dh eine Darlegung der wichtigsten Merkmale. Die SA bringen aber zur konkreten Implementierung nur bedingt Klarheit. Denn diese Informationen könnten sowohl mit Fokus auf die Einzelentscheidung (lokal) oder losgelöst von dieser über alle Entscheidungen hinweg (global) dargelegt werden.

So werden in den SA beispielhaft und nur am Rande „Beispiele für ähnliche Verarbeitungen, die zu Vergleichszwecken anonymisiert bereitgestellt werden“ genannt, die der „Person ein besseres Verständnis der automatisierten Entscheidung ermöglichen, der sie unterworfen worden ist.“[239] Es würde sich dabei um eine Form der beispielbasierten Erklärung handeln, die jedoch gerade nicht auf die konkrete Entscheidung eingeht, sondern durch Zeigen von ähnlichen Beispielen Rückschlüsse ermöglichen will.[240]

Nachdem die SA stark auf das Element der Kontextualität und Nützlichkeit der Information für den Betroffenen sowie in der Formulierung teilweise auf die konkrete Entscheidung (zB “zur fraglichen automatisierten Entscheidung“) abstellen, erscheint eine lokale, auf den konkreten Fall bezogene, Erklärung stärker geeignet, diese Anforderungen zu erfüllen. Im Ergebnis scheint in den SA eine kombinierte Erklärung aus allgemeinen Informationen (Funktionsweise des Mechanismus) sowie Informationen zur konkreten Entscheidung (des Ergebnisses) vorgezeichnet.[241]

Am 27. Februar 2025 folgte das Urteil in der Rechtssache *Dun und Bradstreet*.[242] Der Gerichtshof wies dabei zunächst auf die Mehrdeutigkeit des Wortes „aussagekräftige“ und die Komplementarität der verschiedenen Sprachfassungen hin.[243] Auch der Begriff „involvierte Logik“ würde ein breites Spektrum an Logik umfassen.[244] Primär aus diesem Vergleich der unterschiedlichen Sprachfassungen leitete der EuGH sodann ab, dass unter „involvierter Logik“ „alle Informationen zu subsumieren [sind], die für das Verfahren und die Grundsätze der automatisierten Verarbeitung personenbezogener Daten zum Erreichen eines bestimmten Ergebnisses auf der Grundlage dieser Daten maßgeblich sind“.[245]

Wie auch in den SA wird auf die Rolle des Transparenzprinzips, verkörpert auch in Art 12

[238] *Kelder*, CK v Dun & Bradstreet Austria (C-203/22). The case that ends the GDPR right to explanation debate? https://digi-con.org/ck-v-dun-bradstreet-austria-c-203-22-the-case-that-ends-the-gdpr-right-to-explanation-debate/ (Stand 6. 11. 2024).
[239] SA GA *de la Tour* 12. 9. 2024, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:745, Rz 78.
[240] *Kelder*, CK v Dun & Bradstreet Austria (C-203/22). The case that ends the GDPR right to explanation debate? https://digi-con.org/ck-v-dun-bradstreet-austria-c-203-22-the-case-that-ends-the-gdpr-right-to-explanation-debate/ (Stand 6. 11. 2024).
[241] *Kelder*, CK v Dun & Bradstreet Austria (C-203/22). The case that ends the GDPR right to explanation debate? https://digi-con.org/ck-v-dun-bradstreet-austria-c-203-22-the-case-that-ends-the-gdpr-right-to-explanation-debate/ (Stand 6. 11. 2024).
[242] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117.
[243] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 40 f.
[244] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 42.
[245] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 43.

DSGVO, verwiesen, und konkretisiert, dass „‘aussagekräftige Informationen über die involvierte Logik’ einer automatisierten Entscheidungsfindung im Sinne dieser Bestimmung **alle maßgeblichen Informationen zum Verfahren und zu den Grundsätzen** der automatisierten Verarbeitung personenbezogener Daten **zwecks Erreichen eines bestimmten Ergebnisses** umfassen und diese Informationen aufgrund des Transparenzerfordernisses außerdem in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln sind.“[246]

Das Urteil betont auch den Konnex zwischen Art 15 und den im Falle einer automatisierten Entscheidungsfindung nach Art 22 Abs 3 DSGVO zustehenden Rechten: „Insbesondere im speziellen Kontext des Erlasses einer Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung beruht, bezweckt das Recht der betroffenen Person, die in Art. 15 Abs. 1 Buchst. h DSGVO genannten Informationen zu erhalten, hauptsächlich, ihr die wirksame Ausübung der ihr nach Art. 22 Abs. 3 DSGVO zustehenden Rechte zu ermöglichen, nämlich des Rechts auf Darlegung ihres eigenen Standpunkts und des Rechts auf Anfechtung der Entscheidung.“[247] Denn wenn „von einer automatisierten Entscheidung [...] betroffene Personen nicht in der Lage wären, vor der Darlegung ihres Standpunkts oder der Anfechtung der Entscheidung die Gründe für diese Entscheidung nachzuvollziehen, würden diese Rechte ihren Zweck, diese Personen gegen die besonderen Risiken für ihre Rechte und Freiheiten zu schützen [...] nicht in vollem Umfang erfüllen [...]“.[248] Das Urteil bestätigt auch, mit Verweis auf ErwGr 71 DSGVO, dass Art 15 Abs 1 lit h DSGVO der betroffenen Person ein „**echtes Recht auf Erläuterung der Funktionsweise des Mechanismus** der automatisierten Entscheidungsfindung, der diese Person unterworfen ist, und des Ergebnisses, zu dem diese Entscheidung geführt hat“ bietet.[249]

Schlussendlich kommt der Gerichtshof zum Schluss, „dass das Recht auf ‘aussagekräftige Informationen über die involvierte Logik’ bei einer automatisierten Entscheidungsfindung im Sinne dieser Bestimmung als ein Recht auf Erläuterung des Verfahrens und der Grundsätze zu verstehen ist, die bei der automatisierten Verarbeitung der personenbezogenen Daten der betroffenen Person zur Anwendung kamen, um auf der Grundlage dieser Daten zu einem bestimmten Ergebnis – etwa einem Bonitätsprofil – zu gelangen.“[250] Die relevanten Informationen müssten dabei in präziser, transparenter, verständlicher und leicht zugänglicher Form übermittelt werden.

Das Urteil stellt dabei, wie auch in den SA, klar, dass dieses Telos weder durch die „die bloße Übermittlung einer komplexen mathematischen Formel (etwa eines Algorithmus), noch die detaillierte Beschreibung jedes Schritts einer automatisierten Entscheidungsfindung“ erreicht werden könne, „da beides keine ausreichend präzise und verständliche Erläuterung darstellt.“[251] Dieses Spannungsverhältnis zwischen Transparenz und Erläuterung wird erneut

[246] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 50 (Hervorhebungen durch die Autor:innen).
[247] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 55.
[248] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 56.
[249] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 57 (Hervorhebungen durch die Autor:innen).
[250] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 58.
[251] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 59.

vom EuGH aufgegriffen: „Die 'aussagekräftigen Informationen über die involvierte Logik' einer automatisierten Entscheidungsfindung im Sinne von Art. 15 Abs. 1 Buchst. h DSGVO müssen also das **Verfahren und die Grundsätze**, die konkret zur Anwendung kommen, so beschreiben, dass die betroffene Person nachvollziehen kann, welche ihrer personenbezogenen Daten im Rahmen der in Rede stehenden automatisierten Entscheidungsfindung auf welche Art verwendet wurden, ohne dass die Komplexität der im Rahmen einer automatisierten Entscheidungsfindung vorzunehmenden Arbeitsschritte den Verantwortlichen von seiner Erläuterungspflicht entbinden könnte."[252]

Der Gerichtshof nennt dabei auch ein Beispiel für die Erfüllung des Auskunftsrechtes, denn er würde es „insbesondere als ausreichend transparent und nachvollziehbar erachten, die betroffene Person zu informieren, in welchem Maße eine Abweichung bei den berücksichtigten personenbezogenen Daten zu einem anderen Ergebnis geführt hätte."[253] Diese Form von Erklärung wird im XAI-Bereich häufig als sog. counterfactual oder kontrafaktische Erklärung bezeichnet.[254]

Betreffend diese Vorlagefragen kommt der EuGH zum Schluss, „dass Art. 15 Abs. 1 Buchst. h DSGVO dahin auszulegen ist, dass bei automatisierten Entscheidungsfindungen (einschließlich Profilings) im Sinne von Art. 22 Abs. 1 DSGVO die betroffene Person vom Verantwortlichen im Rahmen des Anspruchs auf Erteilung 'aussagekräftiger Informationen über die involvierte Logik' verlangen kann, ihr anhand der maßgeblichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form **das Verfahren und die Grundsätze zu erläutern, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses [...] konkret angewandt wurden**."[255]

Wie oben zu den SA ausführlicher dargestellt, scheint der EuGH stärker auf das lokale Element, dh die Einzelentscheidung, abzustellen, wobei die Ausführungen einen gewissen Spielraum offen lassen und daher die Frage nach lokalen im Vergleich zu rein globalen Erklärungen nicht abschließend geklärt ist. Als technische Implementierung werden insbesondere Counterfactuals genannt. Im Sinne der Betonung der Kontextualität kann diese Technik in anderen Fällen unseres Erachtens jedoch auch ungenügend sein, um die aussagekräftigen Informationen zu vermitteln.

#### 5.4.2.3 Tragweite und angestrebte Auswirkungen

Das dritte Informationselement, das sich in dieser Form nicht in Art 86 AI Act findet, bezieht sich auf die „Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für

[252] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 61 (Hervorhebungen durch die Autor:innen).
[253] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 62.
[254] ZB *Wachter/Mittelstadt/Russell*, Counterfactual Explanations Without Opening the Black Box. Automated Decisions and the GDPR, Harvard Journal of Law & Technology 2018, 841.
[255] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 66 (Hervorhebungen durch die Autor:innen).

die betroffene Person." Die Interpretation dieses Elements eröffnet große Interpretationsspielräume.[256] Sie sind nach *Paal* und *Hennemann* „vergleichsweise konturlos".[257] Es wird daher in der Literatur nur selten näher behandelt.

Nach *Haidinger* „empfiehlt sich, Tragweite und Auswirkungen möglichst lebensnah zu beschreiben, zB bei Versicherungsprämien, die vom Fahrverhalten abhängig sind, zu erklären, dass ein gefährliches Fahrverhalten höhere Versicherungsprämien zur Folge haben kann".[258]

Auch die A29WP führt aus, dass, damit diese Informationen aussagekräftig und verständlich sind, echte, greifbare Beispiele für die Art der möglichen Auswirkungen genannt werden sollten. Verantwortliche könnten im digitalen Kontext zusätzliche Instrumente nutzen, um Auswirkungen zu verdeutlichen (bei der automatisierten Festlegung von Versicherungsprämien für Kraftfahrzeuge, die auf der Überwachung des Fahrverhaltens der Kund:innen basieren, könnte bspw zur Veranschaulichung erläutert werden, dass gefährliches Fahrverhalten zu höheren Versicherungsgebühren führen kann; dies könnte durch Zurverfügungstellung einer App geschehen, bei der fiktive Fahrer:innen miteinander verglichen werden).[259]

Auch der EuGH, der auf die Leitlinien referenziert, weist als obiter dictum darauf hin, dass „echte, greifbare Beispiele" anzuführen wären und diese Teil des Kontextes der „aussagekräftigen Informationen über die involvierte Logik" wären.[260]

Nach *Dix* muss bspw ein Internetversandhändler seine Kund:innen darüber informieren, dass er ihre bei der Nutzung anfallenden Daten zum Zwecke des Profiling verwendet, um daraus Rückschlüsse auf ihre Bonität zu ziehen und ihnen bei schlechter Bonität Bestellungen nur noch gegen Vorkasse statt auf Rechnung zu gestatten.[261]

Nach *Bäcker*, der Tragweite und angestrebte Auswirkungen synonym interpretiert, muss der Verantwortliche beschreiben, worüber aufgrund der Datenverarbeitung entschieden werden soll, welche Entscheidungsmöglichkeiten bestehen und welche Verarbeitungsergebnisse zu welcher Entscheidung führen oder führen können.

Nach *Kamlah* ist „Tragweite" iSv „Bedeutung" zu verstehen, wodurch den Betroffenen die Möglichkeit gegeben werden soll, zu erkennen, wie der Wahrscheinlichkeitswert einzuschätzen ist. Der bzw die Betroffene soll erkennen können, ob es sich beim Wert um einen guten, mittleren oder schlechten Wahrscheinlichkeitswert handelt (zB über generalisierende Aussagen, wie „überdurchschnittliches" Risiko).[262]

Eine Auskunft über die Tragweite und angestrebten Auswirkungen hat daher möglichst lebensnah zu sein und greifbare Beispiele zu enthalten sowie Betroffenen Informationen zu

---

[256] *Stollhoff* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG[8] (2024) Art 15 DSGVO Rz 23.
[257] *Paal/Hennemann* in *Paal/Pauly*, Datenschutz-Grundverordnung. Bundesdatenschutzgesetz[3] (2021) Art 15 DSGVO Rz 31.
[258] *Haidinger* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 15 DSGVO Rz 46 (Stand 1.12.2021, rdb.at).
[259] *A29WP*, Leitlinien zu automatisierten Entscheidungen im Einzelfall 28 f.
[260] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 45.
[261] *Dix* in *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht. DSGVO mit BDSG (2019) Art 13 DSGVO Rz 16.
[262] *Kamlah* in *Plath*, DSGVO/BDSG/TTDSG[4] (2023) Art 13 DSGVO Rz 29.

liefern, welche Verarbeitungsergebnisse zu welcher Entscheidung führen (können) und wie ein Wahrscheinlichkeitswert einzuschätzen ist.

### 5.4.3 Informationspflichten nach der DSGVO

Die DSGVO enthält verschiedene Regelungen, welche die Transparenz gegenüber Betroffenen adressieren. Zentral sind dabei insbesondere die Art 13 und 14 DSGVO, welche vorgelagerte Informationspflichten von Verantwortlichen gegenüber betroffenen Personen regeln und an dieser Stelle näher ausgeführt werden, da sie später zum Vergleich mit den entsprechenden Bestimmungen des AI Act herangezogen werden (siehe Abschnitt 5.5.7). Der Anwendungsbereich der beiden Bestimmungen differenziert dabei nach der Herkunft der Daten: Während Art 13 DSGVO die Informationspflicht „bei Erhebung von personenbezogenen Daten bei der betroffenen Person“ betrifft, handelt Art 14 DSGVO von der Informationspflicht, „wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden“. Allgemeine Grundsätze dieser Informationspflichten regelt insbesondere auch Art 12 DSGVO, wonach der Verantwortliche geeignete Maßnahmen zu treffen hat, um den betroffenen Personen die Informationen nach den Art 13 und 14 sowie die Mitteilungen nach Art 15 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die beiden Bestimmungen weisen dabei gewisse Unterschiede bzgl den zur Verfügung zu stellenden Informationen auf.[263]

[263] Siehe grundsätzlich *Illibauer* in *Knyrim,* Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 14 DSGVO Rz 11 (Stand 1. 12. 2021, rdb.at) und im Detail auch im Folgenden.

#### 5.4.3.1 Artikel 13 DSGVO

Nach Art 13 Abs 1 DSGVO hat der Verantwortliche Betroffenen zum Zeitpunkt der Erhebung der Daten prinzipiell bereitzustellen:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters; (Abs 1 lit a)
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten; (Abs 1 lit b)
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung; (Abs 1 lit c)
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden; (Abs 1 lit d)
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (Abs 1 lit e) und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind. (Abs 1 lit f)

Anders als bei der Auskunftserteilung nach Art 15 DSGVO muss der Verantwortliche gemäß Art 13 DSGVO selbst aktiv werden und der betroffenen Person eine umfassende Information zukommen lassen.[264]

Nach Abs 2 hat der Verantwortliche zusätzlich folgende Informationen, „die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten“[265] bereitzustellen:

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; (Abs 2 lit a)
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit; (Abs 2 lit b)
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2

[264] Vgl dazu etwa *Däubler in Däubler/Wedde/Weichert/Sommer,* EU-DSGVO und BDSG. Kompaktkommentar³ (2024) Art 13 DSGVO Rz 1.

[265] Das Verhältnis der Absätze 1 und 2 sowohl des Art 13 als auch 14 DSGVO bzw der Zweck der entsprechenden Unterteilung ist nicht ganz klar, läuft aber wohl darauf hinaus, dass die Informationen nach Abs 2 (nur) insoweit zur Verfügung zu stellen sind, als dies notwendig ist, um der betroffenen Person den Umfang der Datenverarbeitung so transparent wie möglich zu erläutern. Nach der A29WP wiederum sind die Informationen nach den beiden Absätzen ohne Unterschied zur Verfügung zu stellen; siehe insgesamt: *Illibauer* in *Knyrim,* Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 13 DSGVO Rz 40 ff (Stand 1. 12. 2021, rdb.at).

Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird; (Abs 2 lit c)

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; (Abs 2 lit d)
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte (Abs 2 lit e) und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. (Abs 2 lit f)

Zwar sind diese Informationen laut ErwGr 60 DSGVO nur zu gewähren, wenn dies für eine faire und transparente Verarbeitung notwendig ist, allerdings sind wenige Fälle denkbar, in denen diese Informationen keinen Beitrag zu einer fairen und transparenten Verarbeitung leisten.[266] Daher wird Unternehmen an mehreren Stellen empfohlen, möglichst alle Informationen nach Abs 2 bereitzustellen, um angesichts der unsicheren Rechtslage keine Sanktion zu riskieren und somit Abs 2 nicht anders als Abs 1 zu behandeln.[267]

Außerdem besagt Art 13 Abs 3 DSGVO: „Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.“ Wann eine solche Zweckänderung zulässig ist, bestimmt sich nach Art 6 Abs 4 DSGVO, der die Weiterverarbeitung von personenbezogenen Daten zu kompatiblen Zwecken regelt.[268] Die Information über die Zweckänderung muss auch die Abwägungskriterien beinhalten, die für den neuen Zweck sprechen, und die Folgen der Zweckänderung umfassen (bspw Änderung der Empfängerkategorie oder Drittlandsübermittlung), da die betroffene Person nur dadurch in der Lage ist, ihre Rechte wirksam geltend zu machen.[269]

#### 5.4.3.2 Artikel 14 DSGVO

Die Transparenz der Datenverarbeitung ist insb dann gefährdet, wenn die Daten nicht bei der betroffenen Person direkt und ohne deren Wissen erhoben wurden.[270] Art 14 DSGVO ist daher

[266] MwN *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO Rz 17.
[267] MwN *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO Rz 17.
[268] Vgl *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO Rz 24.
[269] Vgl *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO Rz 25 f.
[270] Vgl *Däubler in Däubler/Wedde/Weichert/Sommer,* EU-DSGVO und BDSG. Kompaktkommentar³ (2024) Art 14 DSGVO Rz 1.

gewissermaßen eine „[...] Auffangnorm, die nicht nur die Erhebung bei einem Dritten umfasst. Vielmehr deckt sie auch Fälle, in denen der Verantwortliche keine 'Erhebung' vornimmt, weil die betroffene Person oder ein Dritter ihm bestimmte Daten aus eigenem Antrieb übersendet."[271]

Nach Art 14 Abs 1 DSGVO hat der Verantwortliche daher der betroffenen Person folgende Informationen mitzuteilen, wenn „personenbezogene Daten nicht bei der betroffenen Person erhoben [werden]":

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters; (Abs 1 lit a)
- zusätzlich die Kontaktdaten des Datenschutzbeauftragten; (Abs 1 lit b)
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung; (Abs 1 lit c)
- die Kategorien personenbezogener Daten, die verarbeitet werden; (Abs 1 lit d)
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten; (Abs 1 lit e)
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind. (Abs 1 lit f)

Sowie wiederum nach Abs 2 zusätzlich folgende Informationen, „die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten":

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; (Abs 2 lit a)
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden; (Abs 2 lit b)
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit; (Abs 2 lit c)
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird; (Abs 2 lit d)

[271] *Däubler* in *Däubler et al,* EU-DSGVO³ Art 14 DSGVO Rz 2a.

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; (Abs 2 lit e)
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen; (Abs 2 lit f)
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. (Abs 2 lit g)

Art 14 Abs 4 regelt weiters: „Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung."

Zudem legt Art 14 Abs 3 fest, dass der Verantwortliche die Informationen zu folgenden Zeitpunkten erteilen hat:

- unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, (lit a)
- falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, (lit b) oder,
- falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung. (lit c)

#### 5.4.3.3 Zusammenschau der Art 13 und 14 DSGVO

Die Bestimmungen der Art 13 und 14 DSGVO sehen schließlich gewisse Ausnahmen von den Informationspflichten vor, was insbesondere den Fall betrifft, dass die betroffene Person die entsprechenden Informationen bereits hat (in Bezug auf den Normtext des Art 13 DSGVO die einzige Ausnahme).[272] Darüber hinaus soll die Informationspflicht entfallen, wenn die Speicherung oder Offenlegung der Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder sich die Unterrichtung der betroffenen Person als unmöglich erweist bzw mit einem unverhältnismäßigen Aufwand verbunden ist (siehe ErwGr 62 DSGVO).[273] Die Informationen nach Art 13 und 14 DSGVO in Bezug auf automatisierte Entscheidungsfindungen müssen weiters nicht erfolgen, wenn diese keine Nachteile für Betroffene mit sich bringen.

Hinsichtlich der zu erteilenden Informationen über die involvierte Logik ist auch auf die

[272] Siehe im Detail Art 13 Abs 4 bzw Art 14 Abs 5 DSGVO.
[273] Vgl *Däubler* in *Däubler et al,* EU-DSGVO Art 13 DSGVO Rz 31 f und *Däubler* in *Däubler et al,* EU-DSGVO Art 14 DSGVO Rz 22 f.

Verbindung zu dem in Art 12 Abs 1 DSGVO normierten Transparenzgebot zu verweisen, wonach die Informationen in verständlicher, klarer und einfacher Sprache zu erteilen sind. [274] Der Begriff der involvierten Logik ist nicht definiert und auch die Erwägungsgründe enthalten keine Hinweise.[275] Denkbar ist es, sich an den Ausführungen der alten Datenschutz-Richtlinie zu orientieren, welche den Auskunftsanspruch nach Art 12 DSGVO auf den logischen Aufbau der automatisierten Verarbeitung beschränkt.[276] Die Angaben zur involvierten Logik müssen so ausgestaltet werden, dass Betroffene einen Erkenntnisgewinn erlangen, was sich beim Einsatz von komplexen Profiling-Algorithmen als weitgehend ungelöste Aufgabe erweist.[277] Unter Betrachtung von Art 12 Abs 1 DSGVO soll sich die Informationspflicht nicht auf mathematische Algorithmen beziehen, sondern allgemeinverständliche und in einfacher Sprache verfasste Erläuterungen zur Berechnungsgrundlage und der Methodik enthalten.[278] Dies kann dazu führen, dass es – wegen der Komplexität von Algorithmen – zu keiner Offenlegung von mathematischen Algorithmen kommen soll, sondern eine allgemeine, verständliche Beschreibung der Berechnungsgrundlagen und der Methodik erfolgen soll.

Der Verantwortliche hat den von automatisierten Entscheidungsfindungen Betroffenen über die involvierte Logik zu informieren. Dabei kann es sich um die Methoden und Kriterien der Datenverarbeitung handeln – wie etwa die Funktionsweise von Algorithmen, die bei der Bildung von Scorewerten genutzt werden. Geboten scheint eine Erläuterung der involvierten Logik, jedoch nicht eine komplette Offenlegung des Datenverarbeitungssystems. Fraglich ist, wie das Spannungsverhältnis betreffend den Schutz von Geschäftsgeheimnissen des Verantwortlichen aufzulösen ist. Durch rezente EuGH-Judikatur ist jedenfalls in Bezug auf Art 15 DSGVO klargestellt, dass Normen wie §4 Abs 6 DSG, die das Auskunftsrecht grundsätzlich ausschließen, wenn die Auskunft ein Geschäfts- oder Betriebsgeheimnis gefährden würde, unionsrechtswidrig sind.[279] Anders als in Art 15 Abs 1 DSGVO, wird der Schutz von Geschäftsgeheimnissen nur in ErwG 63 DSGVO [und dort nur bzgl des Auskunftsrechts!] erwähnt, jedoch nicht in Art 13 Abs 2 lit f DSGVO verankert.[280]

[274] *Eßer* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG[8] (2024) Art 13 DSGVO Rz 45 ff.
[275] *Kamlah* in *Plath* DSGVO/BDSG/TTDSG[4] (2023) Art 13 DSGVO Rz 28.
[276] *Kamlah* in *Plath* DSGVO/BDSG/TTDSG[4] Art 13 DSGVO Rz 28.
[277] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG. Kommentar[4] (2024) Art 13 DSGVO Rz 55 f.
[278] *Kamlah* in *Plath* DSGVO/BDSG/TTDSG[4] Art 13 DSGVO Rz 29.
[279] EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 75.
[280] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG[4] Art 13 DSGVO Rz 54 f.

## 5.5 Das Recht auf Erklärung im AI Act

**Artikel 86 AI Act**

1. **Personen**, die **von einer Entscheidung betroffen** sind, die der Betreiber auf der Grundlage der Ausgaben eines in **Anhang III** aufgeführten **Hochrisiko-KI-Systems**, mit Ausnahme der in Nummer 2 des genannten Anhangs aufgeführten Systeme, getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre **Gesundheit**, ihre **Sicherheit** oder ihre **Grundrechte beeinträchtigt**, haben das **Recht**, vom Betreiber eine **klare und aussagekräftige Erläuterung** zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten.
2. Absatz 1 gilt nicht für die Verwendung von KI-Systemen, bei denen sich Ausnahmen von oder Beschränkungen der Pflicht nach dem genannten Absatz aus dem Unionsrecht oder dem nationalen Recht im Einklang mit dem Unionsrecht ergeben.
3. Dieser Artikel gilt nur insoweit, als das Recht gemäß Absatz 1 nicht anderweitig im Unionsrecht festgelegt ist.

### 5.5.1 Anwendungsbereich des Artikel 86 AI Act

Art 86 AI Act sieht vor, dass Personen gegenüber dem Betreiber eines Hochrisiko-KI-Systems ein Recht auf Erläuterung der Entscheidungsfindung im Einzelfall zukommt, sofern auf Grundlage der Ausgabe des Systems eine sie betreffende Entscheidung gefällt wurde. Dies setzt voraus, dass der Betreiber seine Entscheidung auf Grundlage der Daten aus seinem Hochrisiko-KI-System getroffen hat. Von diesem Recht bestehen jedoch zahlreiche Ausnahmen. Zunächst ist Art 86 AI Act nur auf Hochrisiko-KI-Systeme gemäß Annex III des AI Act anwendbar, mit Ausnahme der in Punkt 2 genannten kritischen Infrastruktur. Sachlich ist Art 86 AI Act somit beispielsweise auf Hochrisiko-KI-Systeme anwendbar, die zur Emotionserkennung, in der Kreditwürdigkeitsprüfung oder in der Preisbildung in Bezug auf Lebens- und Krankenversicherungen eingesetzt werden. Weiters gelten die in Annex III aufgelisteten Systeme nicht als hochriskant, sofern sie kein signifikantes Risiko für die Gesundheit, Sicherheit oder die Grundrechte von natürlichen Personen darstellen (siehe die Ausnahmeregelung in Art 6 Abs 3 AI Act und die entsprechenden Ausführungen in Abschnitt 5.2.2 des gegenständlichen Berichts). Demnach gelten Systeme aufgrund ihrer mangelnden Beeinflussung der Entscheidungsfindung nicht als hochriskant, da davon ausgegangen wird, dass in diesen Fällen kein erhebliches Risiko für die Gesundheit, Sicherheit und Grundrechte

natürlicher Personen besteht.[281] Dies ist etwa dann der Fall, wenn das System nur eine eng gefasste Verfahrensaufgabe durchführt, zur Verbesserung von zuvor abgeschlossenen menschlichen Tätigkeiten eingesetzt wird, nicht dazu gedacht ist, eine menschliche Bewertung zu ersetzen, oder nur vorbereitende Aufgaben übernimmt. Davon gibt es allerdings eine Gegenausnahme, da gemäß Art 6 Abs 3 AI Act die in Anhang III gelisteten KI-Systeme jedenfalls als hochriskant einzustufen sind, wenn sie ein Profiling natürlicher Personen vornehmen.

Zusammengefasst ist also der Anwendungsbereich von Art 86 AI Act eröffnet, sofern ein Hochrisiko-KI-System gem Anhang III AI Act, das nicht unter die Ausnahme nach Art 6 Abs 3 AI Act fällt und nicht unter Punkt 2 Anhang III AI Act gelistet ist, eine Ausgabe macht, welche die Grundlage einer Entscheidung bildet, die eine natürliche Person betrifft.

## Hochrisiko KI-Systeme

Von den eingangs vorgestellten Use Cases erfüllen folgende die Voraussetzungen, um als Hochrisiko-KI-System eingestuft zu werden:

1. KI-Systeme, die zur Preisbildung bei Lebens- und Krankenversicherungen eingesetzt werden
2. Churn Predictions (sofern in Kombination mit anderen Hochrisiko-KI-Systemen, zB Emotionserkennungssystemen)
3. KI-Systeme zur Erhebung der Bonität mit der Ausnahme von Systemen zur Erkennung von Finanzbetrug.
4. Bzgl der Emotionserkennung können jedenfalls Use Case 4.1 und Use Case 4.2 als hochriskant eingestuft werden (sofern keine verbotene Praktik nach Art 5 AI Act vorliegt). Dies gilt prinzipiell auch für Use Case 4.3, sofern keine Ausnahme nach Art 6 Abs 3 lit b AI Act (Verbesserung von abgeschlossenen Dienstleistungen) vorliegt.

Art 86 AI Act verlangt überdies, dass der Betreiber die Entscheidung “auf Grundlage“ der Ausgabe des Systems treffen muss, während ErwGr 171 AI Act spezifiziert, dass die Entscheidung „überwiegend“ auf der Ausgabe des Systems beruhen muss. Es stellt sich somit die Frage, welchen Einfluss die Ausgabe des KI-Systems haben muss, damit die Entscheidung darauf beruht bzw ob Entscheidungen, die nur zum Teil durch das System vorbereitet werden, nicht darunterfallen.[282] Nach allgemeinen Regeln setzt sich jedoch der Normtext des Art 86 AI

[281] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 86 Rz 3.
[282] Diese Meinung vertreten etwa *Feiler/Forgó*, KI-VO. EU-Verordnung über künstliche Intelligenz. Kommentar (2024) Art 86 Rz 4.

Act gegenüber den nicht rechtlich verbindlichen Erwägungsgründen durch[283], weshalb es als ausreichend angesehen wird, wenn die Ausgaben des KI-Systems für die Entscheidung relevant waren und nicht lediglich eine untergeordnete Rolle gespielt haben.[284] Zusammengefasst kann davon jede wesentliche Beeinflussung der Entscheidungsfindung als erfasst angesehen werden, die eine Auswirkung auf den Inhalt und das Ergebnis der Entscheidungsfindung hat.[285] An dieser Stelle ist hervorzuheben, dass Art 86 AI Act im Unterschied zu Art 22 DSGVO nicht fordert, dass das System die Entscheidung selbst trifft, sondern auch, wenn die Ausgaben des Systems die Grundlage für eine (auch vollständig) menschliche Entscheidung bilden.[286] Ist diese Voraussetzung erfüllt, ist der Anspruch gegenüber dem Betreiber des KI-Systems durchsetzbar, also jene Unternehmen oder Einrichtungen, welche das KI-System in eigener Verantwortung im Rahmen ihrer beruflichen Tätigkeit verwenden.

## Beispiel

Schafft ein Versicherungsunternehmen ein KI-System von einem Dritten an, um dann mithilfe dieses Systems Preisanpassungen für seine Kund:innen zu errechnen, handelt es sich bei dem Versicherungsunternehmen um den Betreiber, gegen den der Anspruch nach Art 86 AI Act zusteht.

Schwieriger zu beurteilen ist der Fall, wenn von einem Unternehmen das KI-System zur Erzeugung einer Ausgabe eingesetzt wird (z.B.: zur Errechnung eines Score-Wertes durch eine Kreditauskunftei) und die Ausgabe dann an ein anderes Unternehmen weitergegeben wird, das dann auf Basis der Ausgabe eine Entscheidung trifft (z.B.: ein Telekomunternehmen, das den Score-Wert über die Bonität von Kund:innen zukauft und dann auf Basis des Wertes eine Entscheidung über die Bonität trifft). Hier fallen die Rollen des Betreibers und des Unternehmens, das die Entscheidung trifft, auseinander. Da jedoch „Score-Werte“ auch Entscheidungen darstellen können, welche die letztendliche Haupt-Entscheidung (zB Ausstellen eines Handyvertrags) vorbereiten, wird das Recht auf Auskunft wohl gegen den Betreiber, also gegen die Kreditauskunftei durchsetzbar sein, welche das KI-System „in eigener Verantwortung verwendet“ (Art 3 Z 4 AI Act). Von welcher Kreditauskunftei das Telekommunikationsunternehmen die „Score-Werte“ zugekauft hat, können Betroffene im Rahmen des Auskunftsanspruchs nach Art 15 DSGVO in Erfahrung bringen.

[283] Vgl EuGH 13. 7. 2023, C-376/20 P, *Kommission/CK Telecoms UK Investments*, ECLI:EU:C:2023:561, Rz 105: „Die Erwägungsgründe eines Unionsrechtsakts sind jedoch rechtlich nicht verbindlich und können weder herangezogen werden, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht […].“

[284] Vgl dazu auch die Diskussion in *Hornung*, Individualrechte in der KI-Verordnung. Die Rechte auf Beschwerde und auf Erläuterung der Entscheidungsfindung im Einzelfall, DuD 2024, 507 (510).

[285] *Anderl/Ciarnau* in *Zankl,* KI-VO. Verordnung über künstliche Intelligenz (Artificial Intelligence Act). Kurzkommentar (2025) Art 85-87 Rz 7.

[286] Vgl etwa *Hornung*, DuD 2024, 507 (510) oder *Anderl/Ciarnau* in *Zankl,* Art 85-87 Rz 7.

In einem nächsten Schritt muss die Entscheidung rechtliche Auswirkungen auf die betroffene Person haben oder diese in ähnlicher Weise erheblich beeinträchtigen, nämlich in ihrer Gesundheit, Sicherheit oder in ihren Grundrechten. Dies bedeutet, dass das Recht auf Erklärung nicht zusteht, wenn die auf Grundlage des Systems getroffene Entscheidung keine signifikanten beeinträchtigenden Auswirkungen auf die betroffene Person hat. In Anlehnung an den Wortlaut des Art 22 DSGVO ist die rechtliche Auswirkung als Begründung, Aufhebung oder Veränderung einer Rechtsposition zu verstehen.[287] Die Frage, ob „rechtliche Auswirkungen" stets im negativen Sinn zu interpretieren sind, oder ob auch positive rechtliche Auswirkungen den Anwendungsbereich von Art 86 AI Act eröffnen, stellt sich hier ebenso wie bei Art 22 DSGVO (siehe Kapitel 5.4.1). Ein Blick in die Erwägungsgründe spricht dafür, dass hier nur negative rechtliche Auswirkungen erfasst sind, da laut ErwGr 171 AI Act das Recht auf Erklärung zusteht, sobald die Entscheidung „Rechtswirkungen entfaltet oder diese Person in ähnlicher Weise beeinträchtigt, und zwar so, dass sie ihrer Ansicht nach ***negative*** Auswirkungen auf ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte hat."[288] In Bezug auf Gesundheit, Sicherheit und Grundrechte ist hier also explizit von negativen Auswirkungen die Rede. Dies gilt, im Gegensatz zur unklaren Situation in Bezug auf Art 22 Abs 1 DSGVO, auch für die englische und französische Sprachfassung des ErwGr. Da diese Auswirkungen in gewisser Äquivalenz zu den rechtlichen Auswirkungen stehen, liegt die Interpretation nahe, hier von rein negativen Auswirkungen auszugehen. Diese Auffassung kann auch darauf gestützt werden, dass der EuGH in seiner Spruchpraxis immer wieder die Bedeutung von Erwägungsgründen in der Auslegung des Normtextes hervorhebt, sofern die Erwägungsgründe der auszulegenden Norm nicht entgegenstehen.[289] Weiters handelt es sich bei Art 86 AI Act - im Unterschied zu Art 22 DSGVO - um keine Verbotsnorm, sondern um einen Rechtsanspruch, der in vielen Teilen der Lehre als *ex post*-Anspruch gesehen wird.[290]

[287] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 13.
[288] Hervorhebungen hinzugefügt.
[289] Vgl EuGH 21. 4. 2023, C-10/23, *Remia Com Impex*, ECLI:EU:C:2024:259, Rz 51: „Nach ständiger Rechtsprechung können die Erwägungsgründe eines Unionsrechtsakts den Inhalt seiner Bestimmungen präzisieren und sind ein wichtiges Auslegungselement, das den Willen des Gesetzgebers erhellen kann […]."
[290] Vgl *Radtke,* Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke, RDi 2024, Rz 353 (Rz 358).

## Erwägungsgrund 171

Betroffene Personen sollten das **Recht** haben, eine **Erklärung zu erhalten**, wenn eine **Entscheidung** eines Betreibers **überwiegend auf** den **Ausgaben** bestimmter **Hochrisiko-KI-Systeme** beruht, die in den Geltungsbereich dieser Verordnung fallen, und wenn diese Entscheidung Rechtswirkungen entfaltet oder diese Personen in ähnlicher Weise wesentlich beeinträchtigt, und zwar so, dass sie ihrer Ansicht nach **negative Auswirkungen auf** ihre **Gesundheit**, ihre **Sicherheit** oder ihre **Grundrechte** hat.

Diese **Erklärung** sollte **klar und aussagekräftig** sein, und sie sollte eine **Grundlage bieten**, auf der die betroffenen Personen ihre **Rechte ausüben** können. Das Recht auf eine Erklärung sollte nicht für die Nutzung von KI-Systemen gelten, für die sich aus dem Unionsrecht oder dem nationalen Recht Ausnahmen oder Beschränkungen ergeben, und es sollte nur insoweit gelten, als es nicht bereits in anderem Unionsrecht vorgesehen ist.

Im Lichte der Ausführungen zu Art 22 DSGVO in Kapitel 5.4.1 bzgl der herausfordernden Abgrenzbarkeit zwischen „positiven“ und „negativen“ Auswirkungen ist dennoch auch in Bezug auf Art 86 AI Act zu empfehlen, den Begriff „rechtliche Auswirkungen“ im Zweifel weiter zu verstehen und daher jede Auswirkung, unabhängig von einer versuchten Kategorisierung als positiv oder negativ, zu erfassen.

Die zusätzliche Anforderung in Art 86 AI Act, dass betroffene Personen durch die Entscheidung in ihrer Gesundheit, Sicherheit oder ihren Grundrechten beeinträchtigt werden müssen, wirft die Frage auf, ab wann von einer „Beeinträchtigung“ auszugehen ist. In der Literatur finden sich Beispiele, wie etwa Entscheidungen über gesundheitliche Versorgungsleistungen als Beeinträchtigung der Gesundheit oder eine Anknüpfung an diskriminierende Unterschiedskriterien und Gruppenzugehörigkeiten als Beeinträchtigung der Grundrechte.[291] In Bezug auf rein finanzielle Nachteile ist fraglich, ob diese auch unter diese Beeinträchtigungen fallen, sofern sie nicht als rechtliche Auswirkungen umfasst sind. Teilweise spricht sich die Literatur dagegen aus[292], allerdings könnte argumentiert werden, dass bestimmte finanzielle Nachteile auch eine Grundrechtsbeeinträchtigung darstellen können. Darüber hinaus ist ErwGr 5 AI Act zu entnehmen, dass auch wirtschaftliche Schäden grundlegende Rechte schädigen können. Es ist wohl darauf abzustellen, welche Art und welcher Umfang des finanziellen Nachteils vorliegt. Anzumerken ist jedenfalls, dass die Formulierung „ihrer Ansicht nach [...] beeinträchtigt“ darauf hindeutet, dass für die Frage nach der Beeinträchtigung die Perspektive der betroffenen Person relevant ist.[293]

[291] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 13.
[292] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 13.
[293] Vgl *Hornung*, DuD 2024, 507 (510); *Metikos/Ausloos*, Law, Innovation, and Technology 2025, iE, und *Anderl/Ciarnau* in *Zankl,* Art 85-87 Rz 9.

## Beispiel

So wird beispielsweise nicht von einer Beeinträchtigung ausgegangen, wenn ein System die Handhabung von Dokumenten und die Speicherung von Informationen optimiert oder die Indexierung, Suche oder Textverarbeitung verbessert.[294]

Ebenso wenig wird davon ausgegangen, dass ein System Grundrechte verletzt, das auf Basis von Emotionserkennung personalisierte Werbung für einen bekannten Online-Mode-Händler schaltet (es sei denn, die Werbung wird über verschiedene Geräte sowie in Form eines stark als belästigend empfundenen „Retargetings" geschalten oder erfolgt in diskriminierender oder stark manipulierender Weise). Weiters erscheint dies etwa bzgl Use Case 4.3.a im Zusammenhang mit der Emotionserkennung in der Werbung unwahrscheinlich, sofern auf Basis dessen lediglich Anpassungen/Verbesserungen an Produkten oder Dienstleistungen vorgenommen werden sollen.

Derartige Systeme können jedoch etwa dann Grundrechte verletzen, wenn einer spielsüchtigen Person auf Basis von Emotionserkennung Werbung für Sportwetten geschaltet wird (vgl Use Case 4.1 in Zusammenhang mit der Emotionserkennung in der Werbung).

Weiters spricht Art 86 AI Act davon, dass betroffenen „Personen" ein Recht auf eine entsprechende Erläuterung der Entscheidungsfindung zukommt. In Hinblick auf den dahingehend offen formulierten Wortlaut des Art 86 AI Act, welcher eben lediglich von „Personen" spricht, ist fraglich, ob das Recht gem Abs 1 nur natürliche oder auch juristische Personen umfasst. Dahingehend gibt es mehrere Argumente.

Der Wortlaut legt zunächst nahe, dass natürliche und juristische Personen gemeint sein könnten, da der AI Act an anderer Stelle explizit natürliche Personen anspricht (vgl etwa Art 26 Abs 11 und Art 27 Abs 1 lit c und d). Zudem könnten manche von der Bestimmung adressierte Aspekte, nämlich rechtliche Auswirkungen und Grundrechtsbeeinträchtigungen, auch auf juristische Personen bezogen werden.[295] In der Literatur wird allerdings auch zu Recht angemerkt, dass im Gegensatz zu Art 86 etwa Art 85 AI Act explizit auf juristische und natürliche Personen gleichermaßen Bezug nimmt. Weiters wird angeführt, dass auch der gewissermaßen mit Art 86 zusammenhängende Art 26 Abs 11 AI Act und der dazugehörige ErwGr 93 nur auf natürliche Personen Bezug nehmen, und unter anderem auf diesen Überlegungen beruhend festgestellt, dass Art 86 nach dem gesetzgeberischen Willen wohl nur auf natürliche Personen abzielt.[296]

---

[294] Vgl *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/ (Stand 24. 4. 2024).
[295] Siehe auch *Hartmann* in *Martini/Wendehorst*, KI-VO Art 86 Rz 12.
[296] Vgl insgesamt *Hartmann* in *Martini/Wendehorst*, KI-VO Art 86 Rz 12, wonach weiters eine zwischenzeitlich im Gesetzgebungsverfahren vorgeschlagene Definition betroffener Personen lediglich auf natürliche Personen (und

Dem ist entgegenzuhalten, dass etwa die von der lit d des Art 27 Abs 1 AI Act adressierten Personen[297] im Laufe des Gesetzgebungsverfahrens in Übereinstimmung mit Art 27 Abs 1 lit c AI Act noch explizit auf natürliche Personen eingeschränkt wurden[298], was eine entsprechende Absicht zur Klarstellung bzw Einschränkung in diesem Bereich unterstreicht. Demnach könnte die Tatsache, dass Art 86 im Gegensatz dazu **nicht** entsprechend eingeschränkt wurde und gegenüber diesen und weiteren Bestimmungen des AI Act **nicht** explizit nur auf natürliche Personen Bezug nimmt, schon auf eine entsprechende gesetzgeberische Absicht für eine offenere Formulierung hindeuten.

Zudem scheint auch die Interpretation von Art 86 AI Act, wonach die Bestimmung einen über die DSGVO hinausgehenden Schutz gewährleistet,[299] in diese Richtung zu deuten. Denn einerseits ist insbesondere die DSGVO und damit auch deren Art 15 und 22 auf betroffene juristische Personen nicht anwendbar[300] und andererseits scheint dahingehend auch ein entsprechender Schutzbedarf im Sinne der allgemeinen Zielsetzungen des AI Act zu bestehen.[301] In dem Zusammenhang wäre zunächst etwa an kleine Unternehmen zu denken, denen aufgrund eines KI-gestützten Kredit-Scorings ein für den Fortbestand des Unternehmens wichtiger Kredit verweigert wird. Insbesondere erscheint es in diesem Zusammenhang prinzipiell unzweckmäßig, zwischen einer Ein-Personen-Gesellschaft als Unternehmensträgerin und einer einzelunternehmerisch tätigen, natürlichen Person zu unterscheiden. Allerdings sind im Gegensatz zu Art 86 AI Act letztlich die meisten Listungen des Anhang III explizit nur auf natürliche Personen bezogen, wie auch etwa Z 5 lit b zur Kreditwürdigkeitsprüfung und Bonitätsbewertung. Nichtsdestotrotz könnten manche Fälle des Anhang III durchaus auch juristische Personen betreffen (wie etwa Z 8); zudem könnte Anhang III auch noch geändert werden (vgl Art 7 AI Act).

Vor allem in Hinblick auf eine mögliche weite Auslegung des EuGH im Sinne des *effet utile* ist es demnach wohl empfehlenswert, von der grundsätzlichen Anwendbarkeit des Art 86 AI Act auf juristische Personen auszugehen.

Art 86 Abs 2 AI Act sieht vor, dass das Recht auf Erklärung nicht für Systeme gelten soll, bei denen sich Ausnahmen von oder Beschränkungen der Pflicht nach dem genannten Absatz aus dem Unionsrecht oder dem nationalen Recht im Einklang mit dem Unionsrecht ergeben. Hier kommen sachliche bzw sektorale Ausnahmen oder inhaltliche Beschränkungen der Erläuterungspflicht in Betracht, wobei in beiden Fällen die Grenzen des Unionsrechts zu wahren sind.[302]

Art 86 Abs 3 AI Act normiert die Subsidiarität von Art 86 AI Act und stellt klar, dass dieser nur insoweit zur Anwendung kommt, als das Recht auf Erklärung nicht bereits anderweitig im Unionsrecht festgelegt ist. Dies kann als ein Verweis auf das Auskunftsrecht nach Art 15 Abs

*Personengruppen*) abgezielt hätte, was allerdings schlussendlich keinen Eingang in den endgültigen Text fand.
[297] Wenngleich nicht die ebenso genannten *Personengruppen*.
[298] Siehe *Fülöp/Poindl* in *Pehlivan/Forgó/Valcke*, AI Act Art 27 Abschnitt 3.3.4.4.
[299] Siehe dazu noch im Folgenden, insbesondere unter 5.5.4.
[300] Vgl Art 2 und 4 Z 1 DSGVO.
[301] Vgl hierzu Art 1 AI Act, auch etwa im Vergleich zu Art 1 DSGVO, der wiederum explizit nur auf natürliche Personen Bezug nimmt.
[302] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 16.

1 lit h iVm Art 22 DSGVO verstanden werden.[303] Inwieweit Art 86 AI Act damit zu einem Lückenfüller für Sachverhalte wird, auf welche die Art 22 und Art 15 Abs 1 lit h DSGVO nicht anwendbar sind, wird unter den Punkten 5.5.3. und 5.5.4. näher ausgeführt.

[303] Vgl *Nannini*, Habemus a Right to an Explanation. So What? A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4896020 (Stand 16. 8. 2024): "Article 86(3) specifies that the RTE applies only to the extent that it is not otherwise provided for under Union law, such as the GDPR's RTE arising from Articles 15(1)(h) and 22(1)."

Abbildung 3: Prüfschema zur Anwendbarkeit des Artikel 86 AI Act

### 5.5.2 Bestandteile der Erklärung

Sofern die Entscheidung also rechtliche Auswirkungen auf die betroffene Person hat oder deren Gesundheit, Sicherheit oder Grundrechte ihrer Ansicht nach beeinträchtigt und kein Ausnahmetatbestand vorliegt, steht der Person das Recht zu, vom Betreiber eine **klare** und **aussagekräftige Erläuterung** zur **Rolle des KI-Systems** im Entscheidungsprozess und zu den **wichtigsten Elementen** der getroffenen Entscheidung zu erhalten.

#### 5.5.2.1 Rolle des KI-Systems an der Entscheidungsfindung

In Bezug auf die zu beauskunftende **Rolle** des KI-Systems im Entscheidungsprozess gestaltet sich die Einordnung recht unproblematisch, da sich die Rolle im Entscheidungsprozess grundsätzlich als „die jeweiligen Verursachungsbeiträge an der Entscheidung von Mensch bzw Maschine beschreiben lässt".[304] Demnach muss erläutert werden, wie die Entscheidung unter **Beteiligung** des KI-Systems zustande gekommen ist, welcher Anteil der Entscheidung durch das System determiniert wurde und welcher Spielraum für eine Korrektur bzw Anpassung der Entscheidung durch menschliche Akteure verblieben ist bzw wie dieser im Einzelfall genutzt wurde.[305] Konkret bedeutet dies, dass es sich hier um ein prozessorientiertes Verständnis handelt, wonach zu erläutern ist, in welcher Entscheidungsphase das KI-System in welcher Form grundsätzlich eingesetzt wird (bspw zur Vorselektion, Kategorisierung, Analyse, etc.), inwiefern und wie maßgeblich es an der Entscheidung beteiligt war und inwieweit eine menschliche Anpassung der Entscheidung möglich war bzw auch tatsächlich stattgefunden hat.[306]

#### 5.5.2.2 Die wichtigsten Elemente der getroffenen Entscheidung

*A. <u>Allgemeines</u>*

Der AI Act konkretisiert nicht, was genau unter den **„wichtigsten Elementen"** der getroffenen Entscheidung zu verstehen ist und lässt daher Spielraum bei der Interpretation dieses Terminus. Im Sinne einer teleologischen Auslegung von Art 86 AI Act kommt der Transparenz über die Entscheidungsprozesse eine Schlüsselrolle zu.[307] Denn um beispielsweise seine Rechte ausüben zu können, worauf auch ErwGr 171 AI Act verweist, muss die betroffene Person jedenfalls die zentralen Schritte und Einflussfaktoren der Entscheidungsfindung bewerten können.[308] Damit bleibt zwar der konkrete Pflichtenkreis dieser Norm immer noch vage, aber einen ersten Orientierungspunkt könnte eine „Je-desto-Formel" bieten: Je gravierender die zu erwartenden Beeinträchtigungen, desto höhere Anforderungen an die

[304] Vgl *Merkle*, Transparenz nach der KI-Verordnung - von der Blackbox zum Open-Book? RDi 2024, 414 (419).
[305] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 15.
[306] Vgl *Anderl/Ciarnau* in *Zankl,* Art 85-87 Rz 10 und *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 15.
[307] Vgl dazu *Hornung*, DuD 2024, 507 (511).
[308] *Hornung*, DuD 2024, 507 (511).

Erklärung.[309]

In Bezug auf die Erläuterung kann zwischen zwei grundsätzlichen Arten unterschieden werden: Einerseits können Erläuterungen eine prozessbasierte Erklärung (*process-based explanation*) enthalten, die Informationen über die Steuerung des eingesetzten KI-Systems im Rahmen der Entwicklung und des Einsatzes umfasst.[310] Die prozessbasierte Erklärung wird oftmals mit der datenschutzrechtlichen Informationspflicht in Verbindung gebracht und als *ex ante*-Betrachtungsweise vor der konkreten Entscheidung aufgefasst. Eng damit verknüpft sind Erklärungen, welche auf die Systemfunktionalität zielen und dabei die Logik, Konsequenzen, Relevanz und generelle Funktionalität des Systems beinhalten. Beispiele einer Erklärung über die Systemfunktionalität sind Erläuterungen zu dem zugrundeliegenden Modell, Klassifikationsstrukturen oder Entscheidungsbäume.[311]

Andererseits können Erläuterungen auch eine ergebnisbasierte Erklärung (*outcome-based explanation*) enthalten, die Informationen darüber geben soll, was im Falle einer bestimmten Entscheidung passiert ist.[312] Diese Erklärungskategorie bezieht sich somit auf den Inhalt einer spezifischen Entscheidung und beinhaltet die wesentlichen Entscheidungsgründe, die individuellen Umstände der Entscheidungsfindung, die Gewichtung von Merkmalen, maschinelle Entscheidungsregeln und Informationen über Profilgruppen.[313] Diese Kategorie adressiert vor allem Personen, die von einer KI-basierten Entscheidung betroffen sind und nimmt damit eine *ex post*-Betrachtungsweise ein, die auch Art 86 AI Act als im Nachhinein zustehender Anspruch innewohnt.[314] Denn eine vorherige Informationspflicht des Betreibers gegenüber natürlichen Personen, die von durch Hochrisiko-KI-Systeme unterstützten Entscheidungen betroffen sind, wird grundsätzlich nicht als von Art 86 AI Act direkt umfasst angesehen.[315] Zwar lassen sich den Erwägungsgründen Indizien entnehmen, dass der Betreiber betroffene Personen über ihr Recht nach Art 86 AI Act vorab aufzuklären hat, so enthält beispielsweise ErwGr 93 AI Act folgenden Verweis: „Betreiber der in einem Anhang dieser Verordnung aufgeführten Hochrisiko-KI-Systeme spielen ebenfalls eine entscheidende Rolle bei der Unterrichtung natürlicher Personen und sollten, wenn sie natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten, gegebenenfalls die natürlichen Personen darüber unterrichten, dass sie Gegenstand des Einsatzes des Hochrisiko-KI-Systems sind. Diese Unterrichtung sollte die Zweckbestimmung und die Art der getroffenen Entscheidungen umfassen. Der Betreiber sollte die natürlichen Personen auch über ihr Recht auf eine Erklärung gemäß dieser Verordnung unterrichten.“ Diese Pflicht zur Unterrichtung über die zustehenden Ansprüche wird allerdings nicht direkt

[309] *Hornung*, DuD 2024, 507 (511).
[310] Vgl *Information Commissioner's Office*/*The Alan Turing Institute,* Explaining decisions made with AI (2022) 23 ff, https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence-1-0.pdf.
[311] Vgl *Kim/Routledge,* Why a Right to Explanation of Algorithmic Decision-Making Should Exist. A Trust-Based Approach, Business Ethics Quarterly 2022, 75 (80) und *Wachter/Mittelstadt/Floridi,* International Data Privacy Law 2017, 78.
[312] Vgl *Information Commissioner's Office*/*The Alan Turing Institute,* Explaining decisions 23 ff.
[313] Vgl *Kim/Routledge*, Business Ethics Quarterly 2022, 75 (78).
[314] Vgl *Radtke,* RDi 2024, Rz 353 (Rz 358).
[315] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 5 und *Merkle*, RDi 2024, 414 (419). Nähere Informationen zu den Informationspflichten im Zusammenhang mit Art 86 AI Act finden sich in Abschnitt 5.5.7.

aus Art 86 AI Act abgeleitet, **sondern als von Art 26 Abs 11 AI Act umfasst angesehen**, welcher ein Recht normiert, über den Einsatz von Hochrisiko-KI-Systemen zur Unterstützung in Entscheidungsprozessen informiert zu werden. Es empfiehlt sich eine weite Auslegung von Art 26 Abs 11 AI Act, die auch die Pflicht umfasst, über das Recht auf Erläuterung nach Art 86 AI Act vorab zu informieren (siehe dazu die näheren Ausführungen in Abschnitt 5.5.7).[316]

### *B. Vergleich mit Vorgängerbestimmung Art 68c [EP-Fassung]*

Bevor auf die konkreten Inhalte der Entscheidung eingegangen wird, empfiehlt sich an dieser Stelle ein Blick in die ursprüngliche Fassung von Art 86 AI Act, der im Kommissionsentwurf noch nicht Bestandteil des AI Act war und auf Vorschlag des EP zunächst als Art 68c in den Text aufgenommen wurde. Denn wenn man den finalen Inhalt von Art 86 AI Act betrachtet, fällt auf, dass dieser gegenüber seiner Vorgängerbestimmung Art 68c AI Act [EP-Fassung] deutlich eingeschränkt wurde. Art 68c Abs 1 AI Act [EP-Fassung] lautete wie folgt:

„Personen, die von einer Entscheidung betroffen sind, die der Betreiber auf der Grundlage der Daten aus einem Hochrisiko-KI-System getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit, ihre Grundrechte, **ihr sozioökonomisches Wohlergehen oder andere Rechte, die sich aus den in dieser Verordnung festgelegten Verpflichtungen** ergeben, beeinträchtigt, haben das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung **gemäß Artikel 13 Absatz 1** zur Rolle des KI Systems im Entscheidungsprozess, zu den wichtigsten **Parametern der getroffenen Entscheidung und zu den zugehörigen Eingabedaten** zu verlangen.“[317]

Weggefallen ist einerseits die Beeinträchtigung des sozioökonomischen Wohlergehens. Der Verweis auf die Transparenzpflicht nach Art 13 Abs 1 AI Act ist ebenso entfallen, da dieser nicht mehr wie in der EP-Fassung einen Gegenverweis auf Art 68c AI Act [EP-Fassung] enthält. Dennoch kann die Verbindung zwischen der in Art 13 AI Act verankerten Transparenzpflicht und dem finalen Art 86 AI Act nicht komplett ausgeklammert werden, da diese der Erfüllung des Rechts auf Erklärung durch den Betreiber zwingend vorausgeht. So wird der Betreiber nicht in der Lage sein, angemessene Informationen über den Entscheidungsprozess zu liefern, wenn das System für ihn selbst nicht hinreichend transparent ist und er dessen Ausgaben nicht angemessen interpretieren kann. Auf die weiteren, für die konkreten Inhalte der Erklärung relevanten, Implikationen des Entstehungsprozesses von Art 86 AI Act wird im Folgenden an den einschlägigen Stellen Bezug genommen.

### *C. Konkrete Inhalte der Erklärung*

In Rekurs auf bereits bestehende Literatur, Ableitungen aus dem Entstehungsprozess von Art 86 AI Act sowie Analogien aus dem Datenschutzrecht können folgende Inhalte jedenfalls als

[316] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 5.
[317] Hervorhebungen durch die Autor:innen.

„wichtigste Elemente“ einer KI-basierten Entscheidung aufgefasst werden:

- Es kann davon ausgegangen werden, dass unter den „wichtigsten Elementen der getroffenen Entscheidung“ zunächst jene Kriterien zu verstehen sind, auf denen die Entscheidung beruht. Diese Entscheidungsgründe sind in einer allgemein verständlichen und nicht zu technischen Weise darzulegen.[318] Unter den „wesentlichen Entscheidungsgründen“ sind **zentrale Einflusskriterien** zu verstehen, die für die Entscheidungsfindung herangezogen werden, zusammengefasst also all jene Informationen über die Daten, auf deren Grundlage eine Entscheidung getroffen wurde.[319] Dazu zählen etwa auch vorgelagerte **Vor-Entscheidungen**, welche die letztliche „Haupt-Entscheidung“ bestimmen (zB Segmentierung von Zielgruppen).[320] Ob dies auch sog **Eingabedaten** umfasst, muss mit einem Blick auf die Vorgängerbestimmung Art 68c AI Act [EP-Fassung] analysiert werden. Dieser enthielt nämlich neben der Rolle des Systems im Entscheidungsprozess noch die zwingende Bekanntgabe der wichtigsten „Parameter“ sowie der „zugehörigen Eingabedaten“ im Unterschied zu den wichtigsten „Elementen“ gem Art 86 AI Act. Die terminologische Verschiebung von „Parameter“ zu „Elementen“ lässt auf eine Erweiterung des geforderten Inhalts schließen, da der Begriff „Parameter“ auf algorithmische bzw technische Größen verweist, während „Elemente“ eine breitere, über technische Aspekte hinausgehende, Interpretation erlaubt.[321] Diese Öffnung wird jedoch zumindest im Hinblick auf die der Entscheidung vorausgehenden Faktoren etwas relativiert, da die noch in Art 68c AI Act [EP-Fassung] enthaltenen „zugehörigen Eingabedaten“ als weiterer Bestandteil der Erklärung nicht mehr im finalen Text vorkommen. Damit kann darauf geschlossen werden, dass diese nicht mehr zu beauskunften sind, was wiederum dem *télos* von Art 86 AI Act drastisch zuwiderlaufen würde. Denn gerade Informationen über die Eingabedaten sind für eine betroffene Person wohl essentiell, da diese wohl wissen möchte, auf Basis welcher sie betreffender Daten eine Entscheidung gefällt wurde. Dies wird auch in der Literatur in Bezug auf den ethischen Einsatz von KI betont, wo beispielsweise *Brey* und *Dainow* (2024) darauf verweisen, dass es immer Mechanismen geben muss, um die Entscheidung selbst sowie die dafür verwendeten Daten gegenüber betroffenen Personen zu erklären.[322] Aber auch aus der finalen Fassung des AI Act kann man ein derartiges Erfordernis aus rechtswissenschaftlicher Perspektive herauslesen. So besagt ErwGr 171 AI Act, dass die Erklärung eine Grundlage bieten soll, auf deren Basis die betroffenen Personen ihre Rechte ausüben können. Dies betrifft insbesondere Erklärungen zu den Eingabedaten, da betroffene Personen wohl keine Folgerechte geltend machen können, wenn ihnen keine Informationen darüber vorliegen, auf Basis welcher Daten die Entscheidung überhaupt getroffen wurde. Das

[318] Vgl *Information Commissioner's Office/The Alan Turing Institute,* Explaining decisions, 21.
[319] Vgl *Information Commissioner's Office/The Alan Turing Institute,* Explaining decisions, 21.
[320] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 15.
[321] Vgl die Definitionen von „Parameter“ und „Element“ im Duden-Online-Wörterbuch: https://www.duden.de/rechtschreibung/Parameter und https://www.duden.de/rechtschreibung/Element (abgerufen am 14. 2. 2025).
[322] Vgl *Brey/Dainow,* Ethics by design for artificial intelligence, AI and Ethics 2024, 1265 (1269).

Gegenargument, dass für eine Information die verarbeiteten Daten betreffend auf das Auskunftsrecht nach Art 15 DSGVO verwiesen werden kann, ist nicht haltbar, da Eingabedaten nicht immer personenbezogen sein müssen, was den Anwendungsbereich der DSGVO ausschließen würde.[323]

- Ebenso ist zu beauskunften, wie diese Daten bzw Einflusskriterien zur Entscheidungsfindung beigetragen haben.[324] Dies betrifft insbesondere die **Gewichtung von Merkmalen/Parametern** bzw die Frage nach dem Einfluss konkreter Daten auf die Entscheidungsfindung, wobei nicht ganz unumstritten ist, ob diese ebenfalls Teil der Auskunft sein müssen. So sieht *Hacker* die sog „feature salience" (die Identifikation, welche Merkmale die Entscheidung am meisten beeinflusst haben) als nicht vom Recht auf Erklärung nach Art 86 AI Act umfasst an, wobei er diesen pauschalen Ausschluss teilweise relativiert und davon ausgeht, dass diese doch zu erläutern sind, sofern sie sich zu den „wichtigsten Elementen" zählen lassen.[325] Da insbesondere die Gewichtung von Parametern bzw eine Erklärung darüber, welche Merkmale die Entscheidung im Wesentlichen beeinflusst haben, Aufschluss über potenzielle Diskriminierungen oder Bias in der konkreten Entscheidungsfindung geben kann, ist hier definitiv (und auch im Sinne der in Art 1 Abs 1 AI Act normierten Zielsetzung des Grundrechtsschutzes durch den AI Act) von einer Zugehörigkeit zu den „wichtigsten Elementen" auszugehen.[326]
- Eine weitere Kategorie betrifft die **Auswirkungen** des Einsatzes eines KI-Systems und dessen Entscheidungen auf Einzelpersonen und die Gesellschaft. Die Auswirkungen der Entscheidung auf betroffene Personen sind zwar in Art 86 AI Act nicht explizit als Bestandteil der Erklärung genannt, allerdings in Art 15 Abs 1 lit h DSGVO. Es ist daher in Zusammenschau dieser Artikel zu empfehlen, die Erklärung über die Auswirkungen der Entscheidung als Bestandteil der „wichtigsten Elemente" der Entscheidung zu werten. Dies ergibt sich darüber hinaus aus dem Schutzzweck der Norm und auch der EuGH folgt in seiner Rsp dem Grundsatz, den Wortlaut einer Norm derart auszulegen, dass dieser die möglichst optimale Wirkungskraft verliehen wird (*effet utile*). Zwar könnte argumentiert werden, dass der Betreiber eines KI-Systems die Auswirkungen einer Entscheidung nicht immer absehen kann, da - wie bereits erörtert - Auswirkungen auch immer eine subjektive Komponente aus Betroffenensicht aufweisen. Dem steht jedoch einerseits entgegen, dass Betreiber gem Art 14 AI Act eine wirksame Aufsicht führen und daher die mit dem Einsatz des Systems einhergehenden Risiken verstehen müssen. Weiters kann in bestimmten Fällen gem Art 27 AI Act die Durchführung einer

[323] Dass gemäß Art 15 DSGVO Eingabedaten jedenfalls beauskunftet werden müssen, lässt sich aus dem in Art 15 Abs 3 DSGVO normierten Recht auf Kopie herauslesen, welcher vorsieht, dass Auszüge aus Datenbanken, Abschriften aller personenbezogener Daten, die Gegenstand der Verarbeitung sind, und teilweise sogar ganze Dokumente zu übermitteln sind, welche (zumindest teilweise) einen Rückschluss auf die Eingabedaten zulassen. Das Recht auf Kopie und dessen Implikationen für die zu übermittelnden Daten wird unter anderem in den Schlussanträgen in der Rs Dun & Bradstreet aufgegriffen und noch einmal gestärkt (Vgl SA GA *de la Tour* 12. 9. 2024, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:745, Rz 40 ff).
[324] Vgl *Information Commissioner's Office*/*The Alan Turing Institute,* Explaining decisions, 21.
[325] Vgl *Hacker*, Comments on the Final Trilogue Version of the AI Act 11, https://ssrn.com/abstract=4757603 (Stand 23. 1. 2024).
[326] Dieser Argumentation folgend: *Anderl/Ciarnau* in *Zankl,* Art 85-87 Rz 10.

Grundrechte-Folgenabschätzung bzw einer Datenschutz-Folgenabschätzung nach Art 35 DSGVO vorgeschrieben sein, wobei sich der Betreiber mit den Auswirkungen des Einsatzes seines KI-Systems auseinandersetzen muss. Überdies spricht das bereits erwähnte Effizienzgebot gegen eine derartige Auslegung und darüber hinaus weist ErwGr 171 AI Act ausdrücklich darauf hin, dass Betroffene auf Basis der Erklärung ihre Rechte ausüben können müssen, wofür die Erklärung über die Auswirkungen einer Entscheidung eine entscheidende Prämisse darstellt.

- Ein weiterer Bestandteil der Erklärung könnte die Offenlegung des dem System zugrunde liegenden algorithmischen Codes sein, sofern dies keine Preisgabe von Betriebs- und Geschäftsgeheimnissen voraussetzt. Da jedoch mit der Offenlegung des algorithmischen Codes oftmals eine derartige Preisgabe verbunden ist, wird in der Regel davon ausgegangen, dass nicht der gesamte Algorithmus und die Funktionsweise offenzulegen sind, sondern vielmehr die algorithmische Gewichtung der wichtigsten Parameter[327] und eine Beschreibung der Systemprozesse bzw wie der eingesetzte Algorithmus grob operiert (bspw ob es sich um ein Machine-Learning-System handelt, etc.). Denn das Vorliegen von Geschäftsgeheimnissen darf nicht dazu führen, dass die Auskunft komplett verweigert wird bzw überhaupt keine diesbezüglichen Informationen übermittelt werden. Wird der Code jedoch offengelegt, sollte die Erklärung darüber geeignet sein, Informationen über die tatsächlichen Bedingungen der Schnittstelle zwischen den Eingaben und Ausgaben von Algorithmen und den zugrundeliegenden Annahmen sowie der Art und Weise, wie Datensätze trainiert und implementiert wurden, zu liefern.[328] Außerdem wird an dieser Stelle das Recht von betroffenen Personen vorgebracht, ordnungsgemäß über die Speicherungs- und Löschungsverfahren sowie die Bedingungen eines etwaig erforderlichen Einwilligungsverfahrens informiert zu werden.[329]

Nicht direkt aus Art 86 AI Act ableitbar, aber jedenfalls zu empfehlen ist eine Erklärung über Verantwortlichkeitsketten, aus der hervorgehen soll, wer an der Entwicklung, Verwaltung und Implementierung des Systems beteiligt ist. Dies sollte auch Informationen darüber beinhalten, an wen man sich für eine menschliche Überprüfung einer Entscheidung wenden kann.[330]

Es ist auf jeden Fall zu beachten, dass unterschiedliche Kontexte und Situationen zu einem unterschiedlichen Erklärungsbedarf führen.[331] Während es beispielsweise für Systementwickler:innen notwendig ist, präzise technische Details über die Funktionsweise eines KI-Systems zu kennen, möchten betroffene Personen wahrscheinlich eher verstehen, welche Faktoren zu einer Entscheidung geführt haben. Betroffene haben daher ein besonderes Interesse an Informationen über den Datenursprung, weshalb ihre Daten verarbeitet wurden, wie das dahinter stehende Modell operiert, welche Faktoren die

[327] Vgl *Anderl/Ciarnau* in *Zankl,* Art 85-87 Rz 10.
[328] Vgl *European Parliamentary Research Service (EPRS)* Artificial Intelligence ante portas. Legal & Ethical Reflections 2, https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf (Stand 19. 3. 2019).
[329] Vgl *European Parliamentary Research Service,* Artificial Intelligence ante portas 2.
[330] Vgl *Information Commissioner's Office*/*The Alan Turing Institute,* Explaining decisions, 21.
[331] Vgl *The Royal Society,* Explainable AI. The basics. Policy briefing (2019) 19, https://ec.europa.eu/futurium/en/system/files/ged/ai-and-interpretability-policy-briefing_creative_commons.pdf.

Entscheidung beeinflussen und warum eine bestimmte Ausgabe erzielt wurde.[332]

### 5.5.3 Formale Aspekte im Zusammenhang mit Art 86 AI Act

Die formalen Aspekte im Zusammenhang mit Art 86 AI Act, bspw die Frist zur Beantwortung von Auskunftsbegehren, die Form der Erklärung oder auch die Frage nach den damit verbundenen Kosten lässt Art 86 AI Act komplett unerwähnt. Es gilt daher, höchstgerichtliche Rechtsprechung in Bezug auf diese Fragen abzuwarten und die nachfolgenden Ausführungen als Empfehlungen zu verstehen, bis diese offenen Fragen eindeutig geklärt sind. Das Recht auf Erklärung gem Art 86 AI Act ist jedenfalls mittels Antrags der betroffenen Person geltend zu machen.

#### 5.5.3.1 Frist

Der AI Act lässt grundsätzlich ungeregelt, innerhalb welcher Frist der Betreiber auf ein Auskunftsbegehren nach Artikel 86 AI Act reagieren muss. Es empfiehlt sich daher eine Analogie mit den entsprechenden Bestimmungen der DSGVO, da betroffene Personen in der Praxis auch beide Rechte auf Auskunft – nämlich jenes nach Artikel 15 DSGVO und jenes nach Artikel 86 AI Act – gleichzeitig geltend machen können und eine unterschiedliche Frist hier nicht zweckmäßig wäre. Art 12 DSGVO stellt hier die entsprechende datenschutzrechtliche Bestimmung dar und legt fest, dass der betroffenen Person die entsprechenden Informationen unverzüglich, in jedem Fall jedoch **innerhalb eines Monats nach Eingang des Auskunftsbegehrens** zur Verfügung zu stellen sind. Bei komplexen Begehren ist es möglich, diese Frist **auf zwei weitere Monate auszudehnen**, worüber die betroffene Person zusammen mit den Gründen für die Verzögerung innerhalb eines Monats nach Einlangen des Auskunftsbegehrens zu informieren ist.

Natürlich sind auch Fälle denkbar, in denen aufgrund der Komplexität des KI-Systems eine Erhebung der relevanten Informationen innerhalb dieses Zeitraums nicht möglich und daher eine längere Frist notwendig ist. Dies wird es wohl im Einzelfall zu prüfen gelten.

#### 5.5.3.2 Form und Kosten der Erklärung

Auch hierzu enthält der AI Act keinerlei Anforderungen, weshalb erneut auf Artikel 12 DSGVO Bezug zu nehmen ist. Demnach sind betroffenen Personen die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zu übermitteln. Die Beantwortung des Auskunftsbegehrens kann in **jeder angemessenen Form** erfolgen, beispielsweise mündlich, schriftlich oder digital. Sofern die betroffene Person den Antrag elektronisch stellt, ist dieser auch nach Möglichkeit auf

[332] Vgl *The Royal Society,* Explainable AI 19.

elektronischem Weg zu beantworten. Weiters ist die Auskunft **kostenlos** zur Verfügung zu stellen, es sei denn, es handelt sich um exzessive oder offenkundig unbegründete Anträge (siehe Art 12 Abs 5 DSGVO).

#### 5.5.3.3 Negativauskunft

Es ist auch denkbar, dass Personen das Recht auf Erläuterung nach Artikel 86 AI Act geltend machen, obwohl ihnen dieses nicht zusteht, weil sie entweder nicht von einer Entscheidung betroffen sind oder eine sie betreffende Entscheidung nicht durch Unterstützung eines erfassten Hochrisiko-KI-Systems gefällt wurde. Auch wenn es nicht dezidiert rechtlich normiert ist, sollte in weiter Auslegung des Art 26 Abs 11 AI Act in diesen Fällen eine Negativauskunft an die anfragende Person erfolgen, also der Verweis, dass gerade keine Entscheidungen auf Grundlage der Ausgaben des KI-Systems getroffen werden sowie dargelegt werden, weshalb Artikel 86 AI Act nicht zur Anwendung kommt. Dies empfiehlt sich einerseits aus Dokumentationszwecken und andererseits im Lichte der Kund:innenfreundlichkeit (Siehe auch Abschnitt 5.5.7).

### 5.5.4 Zur Relevanz von Art 86 AI Act

Es fällt auf, dass, während die DSGVO in den Art 15 ff einen ganzen Katalog von Betroffenenrechten enthält, der AI Act mit Art 86 nur ein einziges vergleichbares – nachgelagertes – Recht für betroffene Personen vorsieht (für mehr Details zu sonstigen – insbesondere vorgelagerten - Informationspflichten, vgl Abschnitt 5.5.7).[333] Zwar normiert Art 85 AI Act ein Recht auf Beschwerde bei einer Marktüberwachungsbehörde und Art 87 AI Act regelt die Meldung von Verstößen und den Schutz von Hinweisgebern, allerdings erschöpfen sich darin auch bereits die gem AI Act zugestandenen Rechtsbehelfe und Art 86 bleibt das einzige unter ihnen, das direkt gegenüber dem Betreiber durchsetzbar ist. Umso begrüßenswerter erscheint es, dass das Recht auf Erklärung, welches im ursprünglichen Verordnungsentwurf der Europäischen Kommission noch nicht vorgesehen war, schließlich auf Bestreben des Europäischen Parlaments in den Text aufgenommen wurde.[334]

[333] *Schwartmann/Köhler*, Rechtsbehelfe, in *Schwartmann/Keber/Zenner* (Hrsg), KI-VO. Leitfaden für die Praxis (2024) Rz 56 (Rz 58).
[334] *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner* Rz 56 (Rz 58).

Dennoch verbleibt in Anbetracht der in Abs 1 und 2 genannten Ausnahmen sowie der in Abs 3 verankerten Subsidiarität nur ein enger Anwendungsbereich dieser Bestimmung.[335] Aus diesem Grund wird der Wert von Art 86 AI Act an manchen Stellen hinterfragt und dies gerade damit begründet, dass der ursprüngliche Verordnungsentwurf das Recht extra ausgeklammert hatte.[336] In Anlehnung an das *explanatory memorandum* der EU-Kommission wird argumentiert, dass das Recht auf Erklärung bereits in anderen Bestimmungen des AI Act angelegt sei – bspw in der Transparenzvorschrift des Art 13 oder durch die in Art 14 verankerte menschliche Aufsicht – weshalb der Anwendungsbereich von Art 86 AI Act limitiert bleibe.[337] Die genannten Vorschriften begründen jedoch keine direkte Verpflichtung des Betreibers, KI-Entscheidungen gegenüber betroffenen Personen zu erläutern, weshalb einem explizit verankerten Recht auf Erklärung große Bedeutung beigemessen werden kann. So kann die Bestimmung betroffenen Personen die Geltendmachung von Folgerechten erleichtern, da – ähnlich zu dem in Art 15 DSGVO verankerten Auskunftsrecht – das Recht auf Erklärung eine Prämisse für die Geltendmachung anderer Rechtsansprüche darstellen kann.[338] Zu denken wäre hier etwa an produkthaftungsrechtliche Ansprüche[339] oder an Rechtsbehelfe gegen die Entscheidung selbst, die im Wesentlichen davon abhängen, dass die betroffene Person Informationen über die Entscheidungsgründe sowie den Entscheidungsprozess vorlegt. Weitere Überlegungen zur Relevanz von Art 86 AI Act stellen sich insbesondere in Abgrenzung zum Auskunftsrecht der DSGVO (siehe sogleich).

### 5.5.5 Abgrenzungsfragen – „Lückenfüller“ Art 86 AI Act?

Ausgangspunkt ist an dieser Stelle die Frage, ob die Subsidiarität von Art 86 AI Act bedeutet, dass dieser generell nicht zur Anwendung kommt, sobald der Anwendungsbereich von Art 22 iVm Art 15 Abs 1 lit h DSGVO eröffnet ist, oder, ob das Recht auf Erklärung nach Art 86 AI Act auch neben den entsprechenden Ansprüchen der DSGVO besteht, sofern der Auskunftsanspruch nach der DSGVO gewisse Dinge nicht abdeckt, die Art 86 AI Act sehr wohl enthält („Lückenfüller-Position“). Für letztere Auslegung spricht der Wortlaut von Art 86 Abs 3 AI Act, der besagt, dass Artikel 86 AI Act nur insofern zur Anwendung kommt, als das „Recht

[335] *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner* Rz 56 (Rz 58).
[336] Vgl bspw *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (Stand 24. 4. 2024).
[337] Vgl bspw *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (Stand 24. 4. 2024).
oder *Panigutti/Hamon/Hupont/Fernandez Llorca/Fano Yela/Junklewitz/Scalz/Mazzini/Sanchez/Soler Garrido/Gomez,* The role of explainable AI in the context of the AI Act, in ACM (Hrsg), FAccT '23. Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency 2023, 1139.
[338] Vgl *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (Stand 24. 4. 2024).
[339] Vgl *Radtke,* RDi 2024, Rz 353 (Rz 358).

gemäß Absatz 1“ nicht anderweitig im Unionsrecht festgelegt ist, womit der Wortlaut eine vollständige Identität auf Tatbestands- und Rechtsfolgenseite zu erfassen scheint.[340] Darüber hinaus wird argumentiert, dass dann von einer Subsidiarität von Art 86 AI Act auszugehen ist, wenn eine „andere gültige und auf den Einzelfall anwendbare Vorschrift für die betroffene Person eine vergleichbare Rechtsfolge herbeiführt“, wobei hier die Merkmale der scheinbar in Konkurrenz stehenden Bestimmungen nicht deckungsgleich seien.[341] Und auch *Metikos* und *Ausloos* vertreten die Auffassung, dass Art 86 AI Act das Auskunftsrecht nach der DSGVO nicht berührt, sondern als „zusätzliches Recht besteht, das individuellen Entscheidungen unterworfene Betroffene neben dem Auskunftsrecht nach der DSGVO ausüben können.“[342] Das Recht nach Abs 1 beinhaltet nämlich nicht idente Elemente wie der Auskunftsanspruch nach Art 15 DSGVO, da sich die Passage „involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung“ aus Art 15 Abs 1 lit h DSGVO nicht zwangsläufig mit der Erläuterung zur „Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen“ gem Art 86 Abs 1 AI Act decken muss. Denn beispielsweise die Rolle des Systems in der Entscheidungsfindung muss laut Art 15 Abs 1 lit h nicht explizit erläutert werden. Weiters spricht Art 22 DSGVO von ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung, während für den Anspruch nach Art 86 AI Act lediglich die Ausgaben des Systems die Grundlage der Entscheidung bilden müssen.[343] Weiters bezieht sich das Recht auf Erklärung auf Hochrisiko-KI-Systeme, während dies für Art 22 DSGVO irrelevant ist.[344] Dies wird auch durch ErwGr 10 AI Act unterstrichen, welcher klarstellt, dass „[…] betroffene Personen weiterhin über alle Rechte und Garantien verfügen, die ihnen durch dieses Unionsrecht gewährt werden, einschließlich der Rechte im Zusammenhang mit der ausschließlich automatisierten Entscheidungsfindung im Einzelfall und dem Profiling.“ Somit regeln Art 86 AI Act und Art 15 Abs 1 lit h iVm Art 22 DSGVO sowohl ihre Voraussetzungen als auch ihre Rechtsfolgen auf unterschiedliche Weise.[345] Daher folgen der gegenständliche Bericht und die Leitfäden der Interpretation, dass beide Rechtsbehelfe parallel nebeneinander bestehen können.[346]

Gegen diese Leseart wird zum Teil ins Treffen geführt, dass der in der EP-Fassung verankerte Art 68c AI Act in Abs 3 noch den expliziten Verweis enthielt, dass das Recht auf Erläuterung unbeschadet der Art 13, 14, 15 und 22 DSGVO gilt, während die finale Fassung diesen Verweis nicht mehr enthält und stattdessen von der Subsidiaritätsklausel ersetzt wurde. Dies lässt eine Tendenz des EU-Gesetzgebers erkennen, beide Ansprüche nicht nebeneinander bestehen lassen zu wollen. Allerdings darf der Entwurfsfassung dieser Norm keine allzu große rechtliche Relevanz in dem Sinn beigemessen werden, als dass sie als eindeutiges Indiz für oder gegen eine bestimmte Interpretation spräche. Es gilt daher eine Klärung dieser strittigen

[340] Vgl *Hornung*, DuD 2024, 507 (511).
[341] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 17 f.
[342] Vgl dazu den englischen Wortlaut in *Metikos/Ausloos,* Law, Innovation, and Technology 2025, iE: “This new provision [Anm: Art 86 AI Act] does not amend the right to an explanation under the GDPR, but rather provides an additional right that individual decision-subjects can exercise besides the right to an explanation under the GDPR.“
[343] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 18.
[344] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 18.
[345] Vgl *Ebers*, Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU’s AI Act, European Journal of Risk Regulation 2024, 1 (13).
[346] Vgl *Anderl/Ciarnau* in *Zankl,* Art 85-87 Rz 12.

Frage durch den EuGH abzuwarten und einstweilen zu empfehlen, im Zweifel von einer Anwendbarkeit des Art 86 AI Act auszugehen.

Ungeachtet dieser eingangs gestellten Abgrenzungsfragen gibt es bestimmte Fälle, in denen die Anwendbarkeit von Art 22 iVm Art 15 Abs 1 lit h DSGVO ausgeschlossen ist und daher – sofern die übrigen Voraussetzungen erfüllt sind – Art 86 AI Act jedenfalls zur Anwendung kommt. Dies einerseits, wenn auf Basis der Ausgabe eines KI-Systems eine Entscheidung getroffen wird, ohne personenbezogene Daten zu verarbeiten. In diesen Fällen ist der Anwendungsbereich der DSGVO generell nicht eröffnet. Dies kann beispielsweise der Fall sein, wenn die Datenverarbeitung auf aggregierten Daten basiert, die keinen Personenbezug mehr enthalten.[347] Weiters gilt Art 22 Abs 1 DSGVO auch nicht in Situationen, in denen zwar personenbezogene Daten verarbeitet werden, der Entscheidungsprozess aber nur teil-automatisiert ist, da Art 22 DSGVO eine „Vollautomatisierung" fordert. Ein Beispiel wäre der Einsatz von Algorithmen zur Betrugserkennung durch öffentliche Stellen, welche verdächtige Personen zwar herausfiltern, die Letztentscheidung allerdings von Sachberbeiter:innen getroffen wird.[348] Mit der Unterscheidung zwischen vollautomatisierten und teilautomatisierten Entscheidungen hat sich der EuGH - wie bereits erläutert - in seinem rezenten *SCHUFA*-Urteil näher auseinandergesetzt und festgestellt, dass die Entscheidungsfindung „maßgeblich" von dem System beeinflusst sein muss, um in den Anwendungsbereich von Art 22 DSGVO zu fallen. Der EuGH in seinem Urteil in Bezug auf die Maßgeblichkeit bei Wirtschaftsauskunfteien:

„Art 22 Abs 1 [DSGVO] […] ist dahin auszulegen, dass eine ‚automatisierte Entscheidung im Einzelfall' im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet."[349]

Die Ausgabe des Systems muss somit die Entscheidung maßgeblich beeinflussen, aber nicht vollständig ersetzen. Selbst wenn dies somit in der Einzelfallprüfung dazu führen kann, dass eine Kombination aus menschlicher und maschineller Entscheidungsfindung in den Anwendungsbereich von Art 22 Abs 1 DSGVO fällt, wird es dennoch einige Kombinationen geben, die nicht von Art 22 Abs 1 DSGVO erfasst sind und Art 86 AI Act zur Anwendung kommt.

Es gibt daher Konstellationen, in denen das Auskunftsrecht nach der DSGVO nicht gilt, betroffene Personen aber dennoch Zugang zu Informationen über KI-Systeme benötigen, mit denen sie in Berührung kommen. An dieser Stelle kommt die Relevanz von Art 86 AI Act

[347] Vgl *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (Stand 24. 4. 2024).
[348] Vgl *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (Stand 24. 4. 2024).
[349] EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 75.

wieder deutlich zum Vorschein, da Betreiber in der Erklärung die Rolle des KI-Systems im Entscheidungsprozess erläutern müssen, was darauf hindeutet, dass das Recht auf Erklärung nach dem AI Act für Entscheidungen gilt, an denen KI-Systeme in verschiedenen Phasen und Funktionen beteiligt sind, von unterstützend bis hin zu vollständig bestimmend. Folglich kann Art 86 AI Act eine wichtige Lücke schließen, die das Recht auf Erklärung nach der DSGVO hinterlässt.[350]

### 5.5.6 Herausforderungen bei der Umsetzung

Das Recht auf Erklärung gilt zwar als Betroffenenrecht, ihm wohnt allerdings auch eine ökonomische Komponente inne, die es nicht außer Acht zu lassen gilt. So kann das Recht auf Erklärung mit den Schutzinteressen der Informationsinhaber:innen in Konflikt geraten und beispielsweise deren Geschäftsgeheimnisse gefährden, da Algorithmen auch als Geschäftsgeheimnisse geschützt sein können. Dies wiederum kann Auswirkungen auf den Wettbewerb zwischen Unternehmen haben, die gerade von der Geheimhaltung ihrer Algorithmen profitieren, womit das Recht auf Erklärung zumindest mittelbar zu einem kartellrechtlichen Instrument werden könnte, da durch die Offenlegung von Algorithmen das Marktungleichgewicht verringert werden könnte.[351] Dieser “trade-off“ zwischen den Interessen der betroffenen Person und der Einrichtung, gegen die das Auskunftsbegehren gerichtet ist, wurde zumindest in Bezug auf Art 15 DSGVO so ausgelegt, dass eine pauschale Auskunftsverweigerung unter Berufung auf Betriebs- oder Geschäftsgeheimnisse unionsrechtswidrig ist, was sich wohl auch auf das Recht auf Erklärung nach Art 86 AI Act übertragen lässt.[352] Eng damit verbunden ist die Konkurrenz von Art 86 AI Act mit dem Urheber- und Patentrecht, deren Schutz Computerprogramme bzw Softwares unterstehen können.[353]

Nicht minder herausfordernd sind die technischen Aspekte, die mit dem Recht auf Erklärung einhergehen. Bei der Umsetzung eines Rechts auf Erklärung ist daher danach zu fragen, wie bestimmte Machine-Learning-Prozesse und Ergebnisse überhaupt erklärt werden können bzw wie der Entscheidungsprozess an sich transparenter gestaltet werden kann.[354] Es ist daher nahezu unmöglich, eine vollständige Erklärung sämtlicher Parameter und Prozesse zu erhalten. Dies ist unter Umständen auch gar nicht notwendig, da der betroffenen Person eine klare und aussagekräftige Erklärung zusteht, auf deren Basis sie ihre Rechte ausüben kann (siehe auch ErwGr 171 AI Act). Von Vollständigkeit ist somit nicht die Rede und eine zu komplexe Erklärung zahlreicher Parameter und Prozesse könnte dies sogar untergraben und nicht mehr nachvollziehbar sein. Daher hindert die fehlende Möglichkeit einer vollständigen

[350] Vgl *Kelder,* On the relative importance of the AI Act right to explanation (2024), https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (Stand 24. 4. 2024).
[351] Vgl *Hoffmann/Kevekordes,* Das Right to Explanation, DuD 2021, 609 (613).
[352] Vgl EuGH 27. 2. 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, Rz 70.
[353] Vgl *Hoffmann/Kevekordes,* DuD 2021, 609 (612).
[354] Vgl *Hoffmann/Kevekordes,* DuD 2021, 609 (614).

XAI die betroffene Person nicht daran, ihr Recht auf Erklärung durchzusetzen.[355]

### 5.5.7 Informationspflichten gem AI Act

Der AI Act enthält noch weitere (teils vorgelagerte) Informationspflichten bzw Transparenzvorschriften, die Betroffenen zugutekommen. Zunächst sind dabei insbesondere die Regelungen in Art 50 sowie 26 Abs 7 und 11 zu nennen.

Artikel 50 regelt Transparenzanforderungen im Zusammenhang mit gewissen KI-Systemen (**nicht notwendigerweise Hochrisiko-Systeme**). So müssen Anbieter etwa grundsätzlich sicherstellen, „dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren“ (Abs 1). Außerdem werden etwa Deepfakes generierende Systeme und solche zur Emotionserkennung (siehe schon 5.3.4) adressiert. In dem Zusammenhang ist auch Art 50 Abs 6 AI Act zu erwähnen, demgemäß die Pflichten in Kapitel III (wozu auch Art 86 zählt) und andere Transparenzpflichten aus dem nationalen oder Unionsrecht (etwa gem DSGVO) von Art 50 Abs 1-4 unberührt bleiben, woraus abzuleiten ist, dass die Transparenzpflichten nach Art 50 klar neben anderen Unionsrechtsakten bestehen und nicht subsidiär gelten.[356] Das ist wohl ein Unterschied von Art 50 AI Act iVm Art 13 f DSGVO zu Art 86 AI Act iVm Art 15, 22 DSGVO, da hier die Subsidiaritätsfrage eindeutiger scheint als bei Art 86.

Demgegenüber regelt Art 26 AI Act grundsätzlich Pflichten von **Betreibern von Hochrisiko-KI-Systemen**.[357] Absatz 7 bezieht sich dabei auf Arbeitgeber als Betreiber solcher Systeme. Diese werden dazu verpflichtet, vor der Inbetriebnahme (siehe Art 3 Z 11 AI Act) oder Verwendung des Systems am Arbeitsplatz „die Arbeitnehmervertreter und die betroffenen Arbeitnehmer darüber“ zu informieren „dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen werden“.

Art 26 Abs 11 bezieht sich hingegen auf Betreiber von in Anhang III gelisteten Hochrisiko-KI-Systemen, „die natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten“, und verpflichtet diese (unabhängig von Art 50) dazu, diese Personen darüber zu informieren, „dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen“. Über automatisierte Entscheidungsfindungen einschließlich Profiling ist prinzipiell auch nach den Informationspflichten gem Art 13-14 DSGVO zu informieren[358], demnach wären bei derartigen Fällen gem Art 22 Abs 1 und 4 DSGVO „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ zur Verfügung zu stellen (Art 13 Abs 2 lit f sowie 14

[355] Vgl *Hoffmann/Kevekordes,* DuD 2021, 609 (615).
[356] Vgl *Martini* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 50 Rz 123 f.
[357] Siehe *Eisenberger* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 26 Rz 1.
[358] Siehe dazu grundlegend *Illibauer* in *Knyrim*, DatKomm Art 13 DSGVO Rz 54 ff mwN, dabei insbesondere auch der EuGH-Rsp zur Rechtssache *Schufa*; *Illibauer* in *Knyrim*, DatKomm Art 14 DSGVO Rz 33.

Abs 2 lit g; siehe auch 5.4.2 und 5.4.3). Zudem wird in Art 26 Abs 11 AI Act auf die Informationspflichten gem Art 13 der DSRL-PJ verwiesen.

Das Recht auf Erläuterung gem Art 86 AI Act wird in Art 26 Abs 11 AI Act zwar nicht explizit genannt, allerdings in ErwGr 93 angesprochen. Demnach sollte die Information „die Zweckbestimmung und die Art der getroffenen Entscheidungen umfassen. Der Betreiber sollte die natürlichen Personen auch über ihr Recht auf eine Erklärung gem dieser Verordnung unterrichten." Es empfiehlt sich daher eine weite Auslegung von Art 26 Abs 11 AI Act, die auch die Pflicht von Betreibern umfasst, über das Recht auf Erläuterung nach Art 86 AI Act vorab zu informieren.[359] Es bleibt jedoch offen, in welcher Form bzw an welcher Stelle und insbesondere zu welchem Zeitpunkt Betroffene über das Recht nach Art 86 AI Act zu informieren sind. In Bezug auf die Platzierung der Information empfiehlt es sich zunächst, Betroffene direkt in der Entscheidungsmitteilung über ihre Rechte zu informieren, aber auch andere Kanäle - vorzugsweise parallel - zu nutzen, um eine höchstmögliche Transparenz zu gewährleisten, wie etwa die Unternehmenswebseite, die Datenschutzrichtlinie oder gedruckte Broschüren. Im Hinblick auf den Zeitpunkt der Information wird man wohl aufgrund des Zwecks der Bestimmungen davon ausgehen müssen, dass die Information vor bzw zum Zeitpunkt der entsprechenden Anwendung des KI-Systems zu erfolgen hat. Dies kann einerseits aus dem Effizienzgebot (*effet utile*) geschlossen werden, da dem Recht auf Erläuterung nach Art 86 AI Act eher eine optimale Wirkungskraft verliehen wird, wenn frühestmöglich über dessen Bestehen informiert wird. Weiters ergibt sich dies aus grundrechtlichen Überlegungen und dem Selbstbestimmungsrecht von Betroffenen, keiner Hochrisiko-KI-gestützten Entscheidung unterliegen zu wollen und daher noch rechtzeitig diesbezügliche Maßnahmen treffen zu können. Jedenfalls ist spätestens in der Entscheidungsmitteilung selbst über die Möglichkeit der Geltendmachung des Rechts auf Erläuterung zu informieren.

Es sind auch Fälle denkbar, in denen die Verarbeitung der Daten bzw die Verwendung des Hochrisiko-KI-Systems, die als Entscheidungsgrundlage dient, und die Entscheidung selbst zeitlich deutlich auseinanderfallen. Als Beispiel wären an dieser Stelle Kund:innengespräche mit der Servicehotline eines Unternehmens zu nennen, wobei anschließend durch Emotionserkennungssysteme, die als Hochrisiko-KI-Systeme gem AI Act einzustufen sind, die Zufriedenheit der Kund:innen pauschal analysiert werden, ohne, dass zunächst konkrete Entscheidungen über die künftige Vorgehensweise in Bezug auf die jeweiligen Kund:innen angedacht sind. Wird nun erheblich später die Entscheidung getroffen, dass die Verträge jener Kund:innen aufgekündigt werden sollen, welche vom KI-gestützten System als „sehr unzufrieden" eingestuft wurden, stellt sich die Frage, zu welchem Zeitpunkt über das Recht nach Art 86 AI Act zu informieren ist, da sich der AI Act zu dieser Frage nicht äußert. Es ist anzunehmen, dass der Einsatz des Hochrisiko-KI-Systems bzw die Verarbeitung der Kundendaten bereits „Vor-Entscheidungen" darstellen, auf deren Basis letztendlich die „Haupt-Entscheidung" getroffen wird. So wurde bspw die Errechnung eines „Creditscores", auf der die Entscheidung über die Kreditwürdigkeit einer Person maßgeblich beruht, im SCHUFA-Urteil des EuGH als vorgelagerte Entscheidung eingestuft, welche die Entscheidung im Hinblick auf die Kreditwürdigkeit bereits wesentlich vorbereitet.[360] Weiters ist anzunehmen, dass sich

[359] Vgl *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 5.
[360] EuGH 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, Rz 44 ff.

Unternehmen dieser Form des KI-Einsatzes gerade aus dem Grund bedienen, später einmal eine Entscheidung auf Basis der dadurch erzeugten Daten zu treffen, die jedenfalls Auswirkungen auf betroffene Personen hat – sei es die Schaltung von personalisierter Werbung, die Preisanpassung bei Lebens- und Krankenversicherung oder die Bonitätsprüfung. Es empfiehlt sich daher, **bereits zum Zeitpunkt der Datenerhebung oder des KI-Einsatzes darüber zu informieren**, dass Hochrisiko-KI-Systeme verwendet werden und mit deren Unterstützung Entscheidungen getroffen werden, welche die Kund:innen betreffen können.

Natürlich kann argumentiert werden, dass zum Zeitpunkt des KI-Einsatzes überhaupt nicht angedacht ist, dessen Ausgaben als Grundlage für eine konkrete Entscheidung heranzuziehen. Dieser Fall ist jedoch etwas realitätsfern, da derartige Systeme wohl zum hauptsächlichen Zweck der Entscheidungsunterstützung eingesetzt werden, und sich weiters eine Abgrenzung, ab wann ein Unternehmen konkret bezweckt, auf Basis einer KI-Ausgabe eine Entscheidung zu treffen, in der Praxis wohl als äußerst schwierig erweisen wird. Daher ist zu empfehlen, im Zweifel so früh und umfassend wie möglich über das Bestehen des Rechts auf Erläuterung nach Art 86 AI Act zu informieren. Dies ergibt sich überdies daraus, dass gem Art 26 Abs 11 AI Act ohnehin bereits zum Zeitpunkt des grundsätzlichen Einsatzes eines entsprechenden Hochrisiko-KI-Systems darüber zu informieren ist, wobei man hier eine Information über das Recht auf Erläuterung nach Art 86 AI Act, das im Falle einer künftigen KI-basierten Entscheidung zustehen würde, ebenfalls anschließen sollte.

Diese Information ist möglichst transparent und auf verschiedenen Kanälen offenzulegen. Im Fall der KI-gestützten Analyse von Kund:innengesprächen mit der Servicehotline eines Unternehmens könnten betroffene Personen bereits zu Beginn des Gesprächs oder über ein automatisiertes Tonband vor Verbindung mit den Kundenbetreuer:innen über dieses Recht aufgeklärt werden. Es ist auch denkbar, Kund:innen in verschiedenen Etappen über einzelne Aspekte der KI-gestützten Entscheidung zu informieren. Zunächst könnte der Einsatz des Hochrisiko-KI-Systems selbst offengelegt und auf die Möglichkeit hingewiesen werden, dass die durch das System generierten Ausgaben künftig als Entscheidungsgrundlage für eine bestimmte Kategorie an Entscheidungen herangezogen werden (inklusive Zweckbestimmung und Art der Entscheidungen iSd ErwGr 93 AI Act) und inwieweit betroffenen Personen in solchen Fällen ein Recht auf Erläuterung nach Art 86 AI Act zukommt. Auch wenn es nicht dezidiert rechtlich normiert ist, sollten hiervon Negativinformationen umfasst sein, also der Verweis, dass gerade keine Entscheidungen auf Grundlage der Ausgaben des KI-Systems getroffen werden. Kommt es letztendlich zu einer konkreten Entscheidung, könnte noch einmal gesondert über die Ansprüche nach Art 86 AI Act informiert werden und es könnten die zu erläuternden Informationen konkret dargelegt werden.

### Beispiel

Wird etwa unter Einsatz eines Hochrisiko-KI-Systems über eine Prämienanpassung bei der Lebensversicherung entschieden, sollte der Betreiber die betroffene Person

bereits zum Zeitpunkt des KI-Einsatzes darüber informieren, dass ein Hochrisiko-KI-System unterstützend in der Berechnung der Prämie tätig ist und auf Basis dieser Berechnung eine Entscheidung über eine Prämienanpassung gefällt werden kann. Es empfiehlt sich zusätzlich, im eigentlichen Schreiben über die Vertragsanpassung erneut auf das Recht nach Art 86 AI Act aufmerksam zu machen.

Findet die Entscheidung digital, beispielsweise auf Online-Portalen durch personalisierte Werbeschaltungen statt, so könnte die Information unmittelbar nach der Entscheidungsmitteilung in Form eines Hyperlinks angezeigt werden.

Grundsätzlich empfiehlt es sich, zeitlich weit vor der eigentlichen Entscheidung über das Recht nach Artikel 86 AI Act zu informieren, beispielsweise durch einen Verweis auf Hochrisiko-KI-gestützte Entscheidungen in der jeweiligen Datenschutzrichtlinie, in etwaigen Transparenzberichten, im FAQ-Bereich auf der Unternehmens-Webseite oder auch in Informationsbroschüren in Filialen des Unternehmens.

Abgesehen von den bisher genannten Pflichten können auch noch weitere Regelungen des AI Act mitunter der Transparenz gegenüber Betroffenen zugutekommen, weshalb es sich empfiehlt, diese Informationen in die Erklärung mit aufzunehmen. In diesem Zusammenhang sind etwa die Registrierungspflichten gem Art 49 AI Act zu nennen, die bestimmte Akteure zur Registrierung verschiedener Aspekte im Zusammenhang mit Hochrisiko-KI-Systemen in der EU-Datenbank gem Art 71 verpflichten. Dies betrifft etwa Zusammenfassungen in Bezug auf Folgenabschätzungen im Zusammenhang mit bestimmten Systemen, die von bestimmten Betreibern zu registrieren sind.[361] Die entsprechend registrierten und in der Datenbank enthaltenen Informationen sollen prinzipiell „auf benutzerfreundliche Weise zugänglich und öffentlich verfügbar“ sein (siehe im Detail, insbesondere zu Ausnahmen, Art 71 Abs 4 AI Act). Weiters kann gem Art 85 prinzipiell „jede natürliche oder juristische Person, die Grund zu der Annahme hat, dass gegen die Bestimmungen dieser Verordnung verstoßen wurde, bei der betreffenden Marktüberwachungsbehörde Beschwerden einreichen“. Derzeit (Stand Februar 2025) wurde noch keine konkrete österreichische Behörde als zuständige Marktüberwachungsbehörde benannt und die Benennung hat bis 2. August 2025 zu erfolgen. Mit 2. November 2024 sind jedoch Behörden und öffentliche Stellen im Grundrechtsbereich mit mehr Befugnissen in Bezug auf KI ausgestattet worden (Vgl 77 Abs 2 AI Act). Diese sind dafür zuständig, die Einhaltung des Unionsrechts zum Schutz der Grundrechte in Bezug auf die in Anhang III genannten Hochrisiko-KI-Systeme zu beaufsichtigen und durchzusetzen (Art 77 Abs 1 AI Act). Die zuständige Marktüberwachungsbehörde treffen dabei umfassende Kooperationspflichten mit den genannten Behörden bzw öffentlichen Stellen.[362] So muss die zuständige Marktüberwachungsbehörde die genannten Einrichtungen über schwerwiegende Grundrechtsvorfälle im Zusammenhang mit Hochrisiko-KI-Systemen informieren und diesen mitteilen, falls sie ein KI-System als Risiko für Grundrechte identifiziert hat (Art 73 Abs 7 und

[361] Siehe im Detail Art 49 Abs 3 und Anhang VIII Abschnitt C AI Act sowie etwa *Fülöp/Poindl* in *Pehlivan/Forgó/Valcke*, AI Act Art 27 Abschnitt 3.3.2 und 3.3.5.
[362] Nähere Details unter: https://www.digitalaustria.gv.at/Themen/KI/Artikel-77-AI-Act.html.

Art 79 Abs 2 AI Act). Stellt die Marktüberwachungsbehörde im Zuge einer Prüfung fest, dass ein Hochrisiko-KI-System trotz seiner Konformität mit dem AI Act ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Grundrechte oder für andere Aspekte des Schutzes öffentlicher Interessen darstellt, so fordert sie unverzüglich den betreffenden Akteur auf, alle geeigneten Maßnahmen zu treffen, um dieses Risiko zu eliminieren. Die zuständige Marktüberwachungsbehörde hat die genannten Einrichtungen im Zusammenhang mit dieser Prüfung zu konsultieren (Art 82 Abs 1 AI Act).

## 5.6 Sanktionen und Schadenersatz

Der AI Act enthält in den Artikeln 99 ff unter dem Titel „Sanktionen“ (Kapitel XII) Strafbestimmungen, die prinzipiell auch Betreiber von KI adressieren (so Art 99 Abs 4 lit e etwa die Pflichten gem Art 26). Hierbei werden aber in Art 99 grundsätzlich bestimmte Pflichten aufgezählt und nicht allgemein jeder Verstoß gegen die Verordnung strafbewehrt. Dabei wird etwa auf Artikel 86 kein Bezug genommen, prinzipiell auch nicht über die Betreiberpflichten gem Art 26 AI Act. Strafbewehrt wäre demnach aber zumindest der in Abschnitt 5.5.6 dargestellte Aspekt der Informationspflicht gem Art 26 Abs 11 AI Act, der sich auf das Recht gem Art 86 bezieht. Ebenso strafbewehrt sind etwa die Transparenzverpflichtungen für Betreiber gem Art 50 AI Act (Art 99 Abs 4 lit g). Grundlegend anders scheint sich dies lediglich in Bezug auf Organe, Einrichtungen und sonstige Stellen der Union zu verhalten, bei denen neben dem Verstoß gegen das Verbot bestimmter Praktiken gem Art 5 AI Act auch jede andere „Nichtkonformität des KI-Systems mit in dieser Verordnung festgelegten Anforderungen oder Pflichten“ sanktioniert werden kann (Art 100 Abs 2 und 3 AI Act).[363] Im Übrigen soll jeder Mitgliedstaat spezifische Regelungen erlassen, „in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können“ (Art 99 Abs 8 AI Act).

Zudem ist darauf zu verweisen, dass die nationale Aufsichtsbehörde gem Art 83 Abs 5 DSGVO bei der Verletzung der Auskunftspflicht bzgl automatisierten Entscheidungen gem Art 15 Abs 1 lit h iVm Art 22 DSGVO ebenso Sanktionen verhängen kann.

Zum aktuellen Zeitpunkt bleibt bis zu einem gewissen Grad noch fraglich, inwieweit zumindest gewisse Regelungen des AI Act, wie auch etwa Art 86, **Schutzgesetze** im Sinne des § 1311 ABGB darstellen (also spezifische, ein Verhalten bereits wegen dessen abstrakter Gefährlichkeit verbietende Rechtsvorschriften) und damit Betroffenen auf dieser Basis Schadenersatzansprüche gegen Personen, die diesen zuwiderhandeln, ermöglichen – freilich unter Beachtung aller (sonstigen) Voraussetzungen.[364] Im Zusammenhang mit KI sind Schutzgesetzverletzungen als Basis für **deliktischen Schadenersatz** generell von besonderer Bedeutung, weil die zu erwartenden Schäden oft nicht absolut geschützte Rechtsgüter betreffen werden (was auch eine Möglichkeit als Grundlage für deliktische Schadenersatzansprüchen wäre) und in Verbindung mit Schutzgesetzverletzungen uU auch solch andere Schäden ersatzfähig sein können.[365]

Dabei ist einerseits hervorzuheben, dass Schadenersatzansprüche nach dem österreichischen Recht grundsätzlich einen gewissen Zusammenhang zwischen dem Schutzzweck der übertretenen Norm und dem geltend gemachten Schaden erfordern, indem nur dann wegen einer Rechtswidrigkeit für einen Schaden einzustehen ist, wenn die verletzte

[363] Vgl grundlegend auch *Anderl/Ciarnau* in *Zankl*, KI-VO (2025) Art 100 Rz 3.
[364] Siehe grundlegend *Karner* in *Bydlinski/Perner/Spitzer*, KBB. ABGB. Kommentar zum ABGB[7] (2023) § 1294 ABGB Rz 1, 4, § 1311 ABGB Rz 3 mwN; siehe weiters grundlegend RIS-Justiz RS0027415 und zu Unionsrecht in diesem Zusammenhang vgl etwa OGH 2. 8. 2012, 4 Ob 46/12m; weiters wäre etwa zu beachten, ob ein ersatzfähiger Schaden vorliegt, vgl dazu, insbesondere im Zusammenhang mit Schutzgesetzen, etwa: *Karner* in *Bydlinski/Perner/Spitzer,* KBB[7] § 1295 ABGB Rz 2 mwN.
[365] Siehe im Detail *Wendehorst* in *Martini/Wendehorst,* KI-VO Art 1 Rz 78 ff.

Norm ebendiesen verhindern sollte (was insbesondere im Zusammenhang mit Schutzgesetzverletzungen praktische Relevanz hat)[366]. Jener Zweck der entsprechenden Normen ist durch teleologische Auslegung zu eruieren.[367] Im gegebenen Zusammenhang ist dabei andererseits wesentlich, dass der AI Act auch keine eigene Haftungsbestimmung, wie etwa Art 82 DSGVO, enthält.[368] In Art 82 DSGVO wird demgegenüber eigenständig eine unmittelbare Haftung aus Delikt für der DSGVO widersprechende Verarbeitungen personenbezogener Daten normiert.[369] *Wendehorst* konstatiert in dem Zusammenhang, dass andere Produktsicherheitsvorschriften oftmals allgemein als Schutzgesetze qualifiziert werden und dass dies zumindest auf manche Vorschriften des AI Act zutreffen dürfte.[370]

In Hinblick darauf ist zunächst festzustellen, dass es ein allgemeiner Zweck des AI Act gem Art 1 Abs 1 ist, „ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte […] vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten“, was einen entsprechenden Schutzgedanken in Hinblick auf Betroffene nahelegt.

Allerdings könnte im Detail zu differenzieren sein, was die genaue Zielrichtung einzelner Regelungen betrifft. Dies folgt etwa auch aus der ursprünglich gewissermaßen in einem Paket mit dem Vorschlag zum AI Act vorgeschlagenen AI Liability Directive (AILD).[371] Diese RL sollte gewisse Beweiserleichterungen quasi ergänzend zu den – prinzipiell dennoch weiterhin – in nationalen bzw (anderen) unionsrechtlichen Vorschriften geregelten außervertraglichen, verschuldensabhängigen, zivilrechtlichen Haftung vorsehen.[372]

In diesem Vorschlag scheint die EU-Kommission (zumindest teilweise) lediglich manche AI Act-(Vorschlag)-Pflichten als „Sorgfaltspflicht, deren unmittelbarer Zweck darin besteht, den eingetretenen Schaden zu verhindern“[373] zu interpretieren, was sich aus einer Zusammenschau des Folgenden ergibt:

Nach dem vorgeschlagenen Text sollten, um eine darin vorgeschlagene Kausalitätsvermutung auszulösen (freilich neben anderen Voraussetzungen), prinzipiell nur Verstöße gegen solche Sorgfaltspflichten einschlägig sein, „deren unmittelbarer Zweck darin besteht, den

[366] Siehe grundlegend *Karner* in *Bydlinski/Perner/Spitzer,* KBB[7] § 1295 ABGB Rz 9, § 1311 ABGB Rz 5 mwN.
[367] Siehe *Karner* in *Bydlinski/Perner/Spitzer,* KBB[7] § 1295 ABGB Rz 9.
[368] Vgl auch *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 1 Rz 61; zum Fehlen eigener spezifischer Haftungsbestimmungen im Vorschlag für den AI Act und zu entsprechenden Haftungserwägungen aus deutscher Perspektive vgl auch *Dötsch*, Außervertragliche Haftung für Künstliche Intelligenz am Beispiel von autonomen Systemen (2022) 400 f.
[369] Siehe im Detail *Schweiger* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 82 DSGVO Rz 1, 38 (Stand 1. 12. 2021, rdb.at).
[370] Vgl *Wendehorst* in *Martini/Wendehorst,* KI-VO Art 1 Rz 84 f.
[371] Der Vorschlag zur AILD wurde allerdings (Stand Februar 2025) noch nicht beschlossen bzw offenbar sogar von der EU-Kommission zurückgezogen (Für nähere Information vgl: https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf).
[372] Vgl Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung/AI Liability Directive [AILD]), COM(2022) 496 final; vgl zur Haftung im Zusammenhang mit künstlicher Intelligenz am Rande zudem die Erläuterungen zur Begründung in: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte, COM(2022) 495 final.
[373] Vgl grundlegend Art 4 Abs 1 lit a AILD-Vorschlag.

eingetretenen Schaden zu verhindern".[374] Weiters sollten dabei hinsichtlich Hochrisiko-KI-Systemen, für die gewisse Anforderungen nach dem AI Act(-Vorschlag) gelten, jedenfalls in Hinblick auf deren Anbieter bzw Personen, die Anbieter-Pflichten gem AI Act(-Vorschlag) unterliegen, wiederum nur bestimmte, abschließend (arg: „nur") aufgezählte Anforderungen nach dem AI Act-Vorschlag einschlägig sein.[375] ErwGr 22 AILD-Vorschlag nannte zudem explizit regulatorische Erfordernisse, die nicht auf einen Schutz vor entsprechenden Schäden abzielen sollen (was sich wohl insbesondere auch auf den AI-Act-Vorschlag beziehen sollte[376]), indem dieser festhielt: „Verstöße gegen Sorgfaltspflichten, deren unmittelbarer Zweck nicht darin besteht, den eingetretenen Schaden zu verhindern, führen nicht zur Geltung der Vermutung; wenn beispielsweise ein Anbieter die erforderlichen Unterlagen nicht bei den zuständigen Behörden einreicht, würde dies bei Schadensersatzansprüchen aufgrund von Personenschäden nicht zur Geltung der Vermutung führen"[377].[378]

Dabei sind allerdings wiederum auch Haftungsszenarien auf Basis von Art 82 DSGVO hervorzuheben, denn dabei wird argumentiert, dass zwar eine Verarbeitung personenbezogener Daten schadensbegründend sein müsse (und nicht etwa bloß eine Informationspflichtverletzung nach Kapitel III DSGVO), dass es daneben aber nicht erforderlich wäre, dass quasi die im Spezifischen verletzte Bestimmung per se den Schutz der Geschädigten bezwecken würde, weil die DSGVO im Gesamten auf den Schutz der Rechte und Freiheiten der betroffenen Personen abziele.[379] Dies könnte dementsprechend prinzipiell in ähnlicher Weise auch in Bezug auf den AI Act argumentiert werden[380], wenngleich anzumerken ist, dass Art 82 DSGVO eben gewissermaßen ein eigenständiges Regime

[374] Vgl ErwGr 22 und Art 4 Abs 1 lit a AILD-Vorschlag.

[375] Vgl ErwGr 26 und Art 4 Abs 2 AILD-Vorschlag; hinsichtlich Nutzern (nunmehr grundsätzlich: *Betreiber*) entsprechender Hochrisiko-KI war die korrespondierende Regelung (Art 4 Abs 3 AILD-Vorschlag) demgegenüber dahingehend nicht so eindeutig, inwieweit die entsprechende Aufzählung von Anforderungen nach dem AI Act-Vorschlag, deren Verletzung für die Kausalitätsvermutung einschlägig wäre, abschließend sein sollte, insbesondere weil dabei kein „*nur*" (oder eine ähnliche Klarstellung) verwendet wurde; zieht man die ErwGr (insbesondere 24 und 26) des AILD-Vorschlags zur Auslegung heran, sollte dieser Regelungsvorschlag aber wohl so zu verstehen sein, dass neben den aufgezählten Anforderungen gem dem AI Act-Vorschlag prinzipiell auch "andere im Unionsrecht oder im nationalen Recht festgelegte Sorgfaltspflichten" für solche Nutzer in Frage gekommen wären, im Hinblick auf den AI Act-Vorschlag aber nur die aufgezählten (vgl ErwGr 26 AILD-Vorschlag, worin unter anderem festgehalten wird, dass die RL Verschulden derartiger Nutzer erfassen sollte, „wenn das betreffende Verschulden in der Nichteinhaltung **bestimmter spezifischer Anforderungen**" gem AI Act(-Vorschlag) bestünde; Hervorhebungendurch die Autor:innen).

[376] Denn unmittelbar davor wurde etwa die Nichteinhaltung einer Gebrauchsanweisung (vgl diesbezüglich insbesondere Art 13 und 29 Abs 1 des AI-Act-Vorschlags; nunmehr prinzipiell Art 13 und 26 Abs 1 AI Act) als potenziell einschlägig angesehen: „Somit kann diese Vermutung beispielsweise bei einem Schadensersatzanspruch aufgrund von Personenschäden gelten, wenn das Gericht feststellt, das [sic] ein Verschulden des Beklagten vorliegt, da dieser eine Gebrauchsanweisung, die eine Schädigung natürlicher Personen verhindern soll, nicht eingehalten hat."; Dies spiegelte sich schließlich auch in Art 4 Abs 3 lit a AILD-Vorschlag wider.

[377] Vgl dazu etwa die Pflichten zur Übermittlung von Unterlagen bereits in Art 23 AI-Act-Vorschlag (nunmehr prinzipiell Art 21 AI Act); vgl in dem Zusammenhang allerdings auch ErwGr 25 AILD-Vorschlag, der in Bezug auf einen Verstoß gegen Pflichten zur Dokumenteneinreichung oder Registrierung bei Behörden festhielt, dass diesfalls „*nach vernünftigem Ermessen nicht davon ausgegangen werden* [kann]*, dass er das vom KI-System hervorgebrachte Ergebnis oder die Tatsache, dass das KI-System kein Ergebnis hervorgebracht hat, beeinflusst hat*", was zusätzlich auf die Voraussetzung nach Art 4 Abs 1 lit b AILD-Vorschlag abgezielt haben dürfte.

[378] Vgl, ähnlich im Hinblick auf die Schutzgesetznatur von AI Act-Vorschriften, erneut: *Wendehorst* in *Martini/Wendehorst,* KI-VO Art 1 Rz 84 f.

[379] Vgl *Schweiger* in *Knyrim*, DatKomm Art 82 DSGVO Rz 38.

[380] Siehe zur allgemeinen Zielrichtung des AI Act, insbesondere gem Art 1 Abs 1, schon oben.

darstellt (siehe schon oben).

Gerade Artikel 86 AI Act scheint jedoch einen bestimmten Schutz Betroffener, nämlich insbesondere durch deren Information, zu bezwecken[381] und könnte damit in gewisser Weise auch auf die Verhinderung entsprechender Schäden abzielen. Weiters war diese Bestimmung im ursprünglichen Vorschlag der Kommission für den AI Act, der schließlich im Zusammenhang mit dem Vorschlag zur AILD maßgeblich war, nicht enthalten und wird demnach dabei auch nicht mitbedacht gewesen sein.[382]

Im Übrigen steht wohl auch die Informationspflicht gem Art 26 Abs 11 AI Act mit dem (Grundrechts-)Schutz Betroffener im Zusammenhang (vgl ErwGr 93 AI Act).

Neben deliktischem Schadenersatz, bzw im Speziellen Schutzgesetzverletzungen, können im Allgemeinen im Zusammenhang mit KI natürlich auch etwa vertragliche Schadenersatzansprüche relevant sein.[383]

Schließlich ist auch zu erwähnen, dass der AI Act in den Anhang I der Verbandsklagenrichtlinie[384] aufgenommen wurde (Art 110 AI Act). Diese Richtlinie bezieht sich auf „Verbandsklagen gegen Verstöße durch Unternehmer gegen die in Anhang I enthaltenen Vorschriften des Unionsrechts einschließlich ihrer Umsetzung in nationales Recht, welche die Kollektivinteressen der Verbraucher beeinträchtigen oder zu beeinträchtigen [Anmerkung: Fehler berichtigt] drohen“ (Art 2 Abs 1 Verbandsklagenrichtlinie). In dem Zusammenhang wird einerseits angemerkt, dass das Recht gem Art 86 AI Act eine spezielle Eignung für die kollektive Rechtsdurchsetzung hätte und andererseits Schadenersatzklagen auf Basis von Schutzgesetzverletzungen wohl die höchste ökonomische Relevanz hätten.[385]

[381] Vgl in diesem Zusammenhang neben dem Normtext von Art 86 AI Act insbesondere ErwGr 171 AI Act und hierzu auch *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 Rz 1 f; vgl auch ErwGr 93 AI Act, vor allem im Zusammenhang mit der entsprechenden Information Betroffener.
[382] Vgl dazu insgesamt die Ausführungen oben (5.5.2) und grundlegend auch die Erläuterungen in der Begründung zum AILD-Vorschlag.
[383] Siehe dazu im Detail *Wendehorst* in *Martini/Wendehorst,* KI-VO Art 1 Rz 90 ff.
[384] Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, ABl L 2020/409, 1.
[385] Siehe insgesamt im Detail *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 110 Rz 1 ff.

## 5.7 Vergleich und Subsumtion der Praxisbeispiele

Die bisherigen Ausführungen haben gezeigt, dass eine gemeinsame Betrachtung der datenschutzrechtlichen Aspekte und Art 86 AI Act notwendig ist, um sich einer Klärung der teils noch offenen Fragen rund um das Recht auf Erklärung im Zusammenhang mit KI-gestützten Entscheidungsprozessen anzunähern. Selbst wenn die mangelnde Praxis mit dem AI Act dazu führt, dass es in Bezug auf einige ungeklärte Aspekte des Art 86 AI Act die höchstgerichtliche Rechtsprechung abzuwarten gelten wird, können bereits wertvolle Ableitungen durch die Analyse der datenschutzrechtlichen Literatur und Judikatur getroffenen und dadurch viele Fragen beantwortet werden. Dabei ist jedoch zu betonen, dass die exemplarisch herangezogenen Praxisbeispiele nur einen Teil der möglichen Anwendungsfälle von Art 86 AI Act abbilden und deren rechtliche Analyse auch nach deren konkreter Ausgestaltung variieren kann. Ebenso werden das Erscheinen vertiefender Literatur sowie die Interpretation von Art 86 AI Act durch die Rechtsprechung dazu beitragen, die rechtliche Subsumtion nachzuschärfen und teils (noch) strittige Fragen zu klären. Die Analyse ist daher keinesfalls als abschließend oder gar rechtsverbindlich zu betrachten, sondern stellt eine erste Annäherung an die praktischen Implikationen des Rechts auf Erklärung nach Art 86 AI Act dar, wobei teilweise auch je nach gewählter Argumentationslinie bzw Interpretation andere Schlussfolgerungen denkbar sind. Im Hinblick auf die ausgewählten Fallbeispiele ergibt sich daher das sogleich zusammengefasste Bild. Folgende Use Case wurden dazu herangezogen:

- **Use Case 1:** Preisbildung in der Lebens- und Krankenversicherung
- **Use Case 2:** KI-basierte Vorhersagen von Kundenabwanderungen, sog „Churn Predictions“
- **Use Case 3:** Bonitäts- und Kreditwürdigkeitsprüfung
- **Use Case 4:** Emotionserkennung im Marketing bzw zur Absatzförderung
    - **Use Case 4.1:** Einsatz von Gestenerkennung zur Feststellung von Reaktionen in der Sportwettenwerbung zu deren Effizienzsteigerung
    - **Use Case 4.2:** Einsatz von Emotionserkennung anhand von Aufnahmen des Gesichtsbereichs im Rahmen der Überprüfung der Identität (etwa bei Flugbuchungen), wobei auf erkannte Emotionen entsprechend reagiert wird (zB mittels sinkender Preise), um die Wahrscheinlichkeit für einen Kauf zu erhöhen
    - **Use Case 4.3:** Einsatz von Emotionserkennung im Marketing für Waren oder Dienstleistungen, um zu erkennen, inwieweit diese angepasst werden könnten (etwa um die Zufriedenheit von Kund:innen zu erhöhen), zB in Form der Anpassung von Reiseangeboten anhand emotionaler Reaktionen auf entsprechende Werbevideos (**Use Case 4.3.a**) oder der Emotionsableitung auf der Basis von Texten oder Audiofiles mit Stimmaufnahmen, um die Zufriedenheit von Bestandskund:innen zu analysieren und darauf zu reagieren (**Use Case 4.3.b**)

### 5.7.1 Relevante Bestimmungen der DSGVO

Der Anwendungsbereich der DSGVO ist eröffnet, sofern personenbezogene Daten iSd Art 4 Abs 1 DSGVO (bspw Name, Adresse, Geschlecht, etc.) verarbeitet werden, was im Wesentlichen auf alle Use Cases zutrifft, ausgenommen etwa Fälle, in denen anonyme Daten verarbeitet werden. In Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten ("sensible Daten") nach Art 9 Abs 1 DSGVO gestaltet sich die Situation je nach Use Case schon etwas differenzierter, da es darauf ankommt, ob bestimmte Datenkategorien wie Daten über die Herkunft, das Sexualleben, die Gesundheit oder die Religion einer Person verarbeitet werden. Während dies im Hinblick auf die Use Cases 1-3 leicht im Einzelfall beantwortet werden kann und davon abhängt, welche Daten genau verarbeitet werden, ist dieses Kriterium für Use Case 4 zur Emotionserkennung schwieriger zu beurteilen:

- Use Case 1: Sensible Daten werden verarbeitet, sofern die Entscheidung über die Gesundheitsrisikofaktoren und in weiterer Folge über die Preisbildung auf Basis der Verarbeitung von Gesundheitsdaten getroffen wird, was in diesem Fall sehr wahrscheinlich ist.
- Use Case 2: Hier kommt es auf den konkreten Fall an, jedoch besteht die Möglichkeit einer Verarbeitung sensibler Daten, wenn aus diesen Daten die Wahrscheinlichkeit einer Kundenabwanderung abgeleitet wird. Dies erscheint jedoch höchst unwahrscheinlich.
- Use Case 3: Auch hier kommt es auf die konkrete Fallkonstellation an, jedoch besteht die Möglichkeit einer Verarbeitung sensibler Daten, wenn aus diesen Daten die Bonität bzw Kreditwürdigkeit abgeleitet wird.
- Use Case 4: Emotionserkennung geht regelmäßig mit der Verarbeitung biometrischer Daten einher, wobei bezugnehmend auf die in Abschnitt 5.3.4 geführte Diskussion darauf abzustellen ist, wie der Begriff "biometrische Daten" auszulegen ist, und ob die Emotionserkennung biometrische Daten nach dem Verständnis der DSGVO – im Unterschied zum AI Act – umfasst, die eine eindeutige Identifizierung betroffener Personen ermöglichen bzw bestätigen. In diesem Fall würden sensible Daten im Sinne der DSGVO vorliegen.
    - Unterfall 4.1: Sofern biometrische Daten verarbeitet werden, welche die eindeutige Identifizierung der betroffenen Person ermöglichen oder bestätigen, ist dies aus DSGVO-Perspektive zu bejahen. In diesem Unterfall ist jedoch die Verarbeitung biometrischer Daten im Sinne der DSGVO tendenziell zu verneinen.
    - Unterfall 4.2: Sofern biometrische Daten verarbeitet werden, welche die eindeutige Identifizierung der betroffenen Person ermöglichen oder bestätigen, ist dies aus DSGVO-Perspektive zu bejahen. In diesem Unterfall werden in aller Regel wohl biometrische Daten im Sinne der DSGVO vorliegen.
    - Unterfälle 4.3.a und 4.3.b: Sofern biometrische Daten verarbeitet werden, welche die eindeutige Identifizierung der betroffenen Person ermöglichen oder

bestätigen, ist dies aus DSGVO-Perspektive zu bejahen. In diesen Unterfällen muss keine Verarbeitung biometrischer Daten im Sinne der DSGVO zwingend vorliegen.

In einem nächsten Schritt gilt es zu analysieren, inwieweit die einzelnen Use Cases in den Anwendungsbereich von Art 22 DSGVO fallen, wovon in weiterer Folge abhängt, ob der Auskunftsanspruch nach Art 15 Abs 1 lit h DSGVO zusteht. Art 22 DSGVO fordert, dass eine auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung getroffen wird, die gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. In den meisten Fällen trifft auch dies auf alle Use Cases zu, wobei es von der Erfüllung der einzelnen Kriterien in den unterschiedlichen Konstellationen abhängt, ob der Anwendungsbereich von Art 22 DSGVO eröffnet ist.

- Use Case 1: Der Anwendungsbereich von Art 22 DSGVO ist eröffnet, da hier automatisiertes Profiling erfolgt, auf dessen Basis eine Entscheidung über die Preisbildung getroffen wird. Weiters entfaltet die auf dem Profiling basierende Entscheidung der Preisanpassung Wirkung gegenüber der betroffenen Person, einerseits auf ihre finanzielle Lage und andererseits im weitesten Sinn auf deren Zugang zu Gesundheitsleistungen. Geht mit der Entscheidung über die Preisanpassung darüber hinaus die Begründung, Auflösung oder Anpassung eines Vertragsverhältnisses einher, ist ohnehin von einer rechtlichen Wirkung auszugehen.
- Use Case 2: Hier kommt es auf den konkreten Fall an, wobei dies zu bejahen ist, sofern hier Profiling von einzelnen Personen erfolgt, auf dessen Basis Profile erstellt werden, aus denen abwanderungsgefährdete Kund:innen selektiert werden, woraufhin für diese gezielte Maßnahmen zur Prävention gesetzt werden.
- Use Case 3: Auch hier ist der Anwendungsbereich von Art 22 DSGVO eröffnet, da der Begriff „Entscheidung“ weit auszulegen ist und auch Vor-Entscheidungen, wie die Errechnung eines Score-Wertes, darunterfallen, sofern sie einen maßgeblichen Einfluss auf die Entscheidungsfindung haben. Die Wirkung liegt sodann in der Entscheidung über eine Kreditvergabe oder über den Abschluss eines Vertrages mit der betroffenen Person.
- Use Case 4: Im Fall der Emotionserkennung ist grundsätzlich davon auszugehen, dass eine Entscheidungsfindung auf Basis einer automatisierten Datenverarbeitung erfolgt. Hinsichtlich des Kriteriums der Auswirkung der jeweiligen Entscheidung ist zu fragen, inwiefern die Entscheidung rechtliche Wirkung entfaltet oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigt.
    - Unterfall 4.1: Insbesondere personalisierte Werbeschaltungen für Sportwetten, die Schwachstellen von Betroffenen ansprechen und ausnutzen, wie beispielsweise die gezielte Werbung für Sportwetten an Spielsüchtige, sind jedenfalls als entsprechende Beeinträchtigung anzusehen.
    - Unterfall 4.2: Hier wird im Einzelfall zu prüfen sein, ob eine ausreichende Beeinträchtigung der finanziellen Gesundheit oder der privaten Lebensführung vorliegt.

- Unterfälle 4.3.a und 4.3.b: Während beim Einsatz von Emotionserkennung in der Werbung zur Anpassung von Produkten und Dienstleistungen wohl noch nicht von einer erheblichen Beeinträchtigung gesprochen werden kann (Unterfall 4.3.a), kann im Fall des Einsatzes von Emotionserkennung zur Analyse der Kundenzufriedenheit, sofern daran eine Entscheidung über bspw die Auflösung eines Vertragsverhältnisses geknüpft wird, eine rechtliche Wirkung angenommen werden (Unterfall 4.3.b).

In den Fällen der Anwendbarkeit von Art 22 DSGVO steht Betroffenen das Recht zu, vom Verantwortlichen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu verlangen. Ungeachtet dessen treffen den datenschutzrechtlich Verantwortlichen in allen Fällen vorab Informationspflichten gem Art 13 bzw 14 DSGVO, welche die Transparenz gegenüber Betroffenen adressieren. Demnach hat der Verantwortliche bestimmte Informationen (seine Kontaktdaten, die Verarbeitungszwecke, die Rechtsgrundlage der Datenverarbeitung, etc.) bereits zum Zeitpunkt der Datenerhebung bereitzustellen.

### 5.7.2 Art 86 AI Act und damit zusammenhängende Bestimmungen

Der Anwendungsbereich des AI Act ist eröffnet, sofern es sich um ein KI-System nach Art 3 Abs 1 AI Act handelt. Es wird im Einzelfall zu prüfen sein, ob das jeweils konkret in einem Unternehmen eingesetzte System diese Anforderungen erfüllt, jedoch ist davon auszugehen, dass dies in den ausgewählten Use Cases regelmäßig zu bejahen sein wird.

In Use Case 4 gilt es darüber hinaus zu fragen, ob ein Emotionserkennungssystem gem Art 3 Z 39 AI Act vorliegt, was unter anderem davon abhängt, ob das System biometrische Daten iSv Art 3 Z 34 AI Act (Daten, die durch eine direkte Messung biologischer Signale zu entsprechenden Personenmerkmalen mittels spezieller technischer Mittel gewonnen werden und auf einen Emotionserkennungszweck abzielen) verarbeitet. Dies muss im jeweiligen einzelnen Anwendungsfall, insbesondere anhand der konkreten technischen Herangehensweise, geklärt werden, wird sich jedoch für die Use Cases 4.1, 4.2 und 4.3.a oftmals bejahen lassen. Lediglich im Hinblick auf Use Case 4.3.b ist das Vorliegen dieser Voraussetzung im Allgemeinen fraglich, soweit nur Texte zur Ableitung von Emotionen verwendet werden, da diesfalls wohl in der Regel keine direkte Messung biologischer Signale vorliegen würde. Werden jedoch bspw Tastaturanschläge oder Gesten analysiert und daraus Emotionen abgeleitet, könnte wiederum eine Emotionserkennung gem AI Act vorliegen. Insbesondere in Bezug auf Use Case 4.1 ist darüber hinaus noch zu prüfen, ob das System auch tatsächlich anhand von Gesten emotionale Reaktionen erkennt, oder ob lediglich andere Zustände oder Gegebenheiten (wie Ermüdung) abgeleitet werden. Im ersten Fall würde es sich um ein Emotionserkennungssystem iSd AI Act handeln, im letzten Fall jedoch nicht.

Die gegenständlichen Use Cases stellen grundsätzlich keine verbotenen Praktiken iSd Art 5 AI Act dar, wobei je nach konkreter Ausgestaltung der Fälle eine Überlappung mit den in Art 5 AI Act gelisteten Verboten möglich ist.

In einem nächsten Schritt ist zu prüfen, ob die in den Use Cases eingesetzten KI-Systeme Hochrisiko-KI-Systeme nach Art 6 Abs 2 iVm Anhang III AI Act darstellen, da Art 86 AI Act nur auf diese anwendbar ist:

- Use Case 1: Ja, da die Preisbildung bei Lebens- und Krankenversicherungen explizit in Anhang III Z 5 lit c AI Act als hochriskant eingestuft ist.
- Use Case 2: Hier handelt es sich grundsätzlich um kein Hochrisiko-KI-System, da es keinem der in Anhang III genannten Bereiche zuzuordnen ist. Sollten Churn Predictions jedoch mithilfe anderer in Anhang III genannten Hochrisiko-KI-Systeme durchgeführt werden, beispielsweise mittels Emotionserkennungssystemen, würde es sich um ein Hochrisiko-KI-System handeln.
- Use Case 3: Systeme, die zur Bewertung der Bonität oder Kreditwürdigkeit natürlicher Personen verwendet werden, gelten als hochriskant iSv Anhang III Z 5 lit b AI Act, mit Ausnahme von KI-Systemen zur Aufdeckung von Finanzbetrug.
- Use Case 4: Hier können, sofern Emotionserkennungssysteme im Sinne des AI Act verwendet werden, insbesondere Use Case 4.1 und Use Case 4.2 nach Anhang III Z 1 lit c AI Act als hochriskant eingestuft werden. Dies gilt prinzipiell auch für Use Case 4.3, sofern keine Ausnahme nach Art 6 Abs 3 lit b AI Act (im Sinne der Verbesserung von abgeschlossenen Dienstleistungen) vorliegt, soweit nicht bereits die Verbote gem Art 5 Abs 1 lit a oder b AI Act einschlägig sind.
- Im Unterfall 4.3.a wird das Vorliegen eines Hochrisiko-KI-Systems allerdings tendenziell zu verneinen sein, da entsprechende Angebote schon im Vorhinein angepasst/verbessert werden, was auch in Unterfall 4.3.b ähnlich wäre, sofern etwa auf eine etwaige Unzufriedenheit direkt mit einem angepassten Angebot reagiert werden würde.

Damit Art 86 AI Act greift, muss weiters vom Betreiber eine Entscheidung auf Grundlage der Ausgabe des Hochrisiko-KI-Systems getroffen werden. Beim Betreiber handelt es sich um jene Einrichtungen oder Unternehmen, die das KI-System in eigener Verantwortung im Rahmen ihrer beruflichen Tätigkeit verwenden. Dies wäre beispielsweise in Use Case 1 das Versicherungsunternehmen oder in Use case 4.3.b das Unternehmen, das mittels Emotionserkennungs-KI Audiomitschnitte von Kundengesprächen analysiert, um die Zufriedenheit der Kund:innen einzuschätzen, und anschließend bestimmte Maßnahmen in Bezug auf als unzufrieden eingestufte Kund:innen ergreift. Die eigentliche Entscheidung ist dabei weit auszulegen, und reicht von „Vor-Entscheidungen“ (bspw Errechnung eines Score-Wertes) über Preisanpassungen bis hin zu allgemeinen Maßnahmen (bspw Werbeschaltungen, die Unterbreitung von Serviceangeboten, etc.). Zentral ist dabei, dass die Ausgabe des KI-Systems relevant für die Entscheidung war und keine lediglich untergeordnete Rolle gespielt hat. All diese Erfordernisse treffen grundsätzlich regelmäßig auf die Use Cases zu.

In einem nächsten Schritt muss die Entscheidung rechtliche Auswirkungen auf die betroffene Person haben oder diese in ähnlicher Weise erheblich beeinträchtigen, nämlich in ihrer Gesundheit, Sicherheit oder in ihren Grundrechten. Dies bedeutet, dass das Recht auf

Erklärung nicht zusteht, wenn die auf Grundlage des Systems getroffene Entscheidung keine signifikanten beeinträchtigenden Auswirkungen auf die betroffene Person hat.

- Use Case 1: Diese Voraussetzung ist bei diesem Use Case strittig, da die Entscheidung hinsichtlich der Preisbildung bei Lebens- und Krankenversicherung einen finanziellen Nachteil darstellt, der nicht als rechtliche Auswirkung gilt und bei dem fraglich ist, ob er eine Grundrechtsbeeinträchtigung darstellt. Es ist jedoch vertretbar zu argumentieren, dass auch bestimmte finanzielle Nachteile (bspw deutlich überhöhte Versicherungsprämien) eine Grundrechtsbeeinträchtigung darstellen. Außerdem wirkt sich die Höhe der Versicherungsprämie in weitestem Sinn auf die Gesundheit aus, da sie den Zugang zu Gesundheitsdienstleistungen betrifft, weshalb auch hier von einer Beeinträchtigung ausgegangen werden kann. Sofern es um die Begründung, die Auflösung, oder die Anpassung eines Vertragsverhältnisses geht, handelt es sich um eine Auswirkung auf die Rechtsposition der betroffenen Person und somit jedenfalls um eine rechtliche Auswirkung.
- Use Case 3: Die Entscheidung über eine Kreditvergabe oder den Abschluss eines Vertrags (bspw Mobilfunk- oder Energielieferungsvertrag) betrifft jedenfalls die Begründung einer Rechtsposition und stellt somit eine rechtliche Auswirkung dar. Darüber hinaus wird es sich in den meisten Fällen um eine relevante Beeinträchtigung handeln, da sich diese Entscheidung auf die finanzielle Lage und die allgemeine Lebenssituation der betroffenen Person auswirkt.
- Use Case 4: Hier gilt allgemein der Grundsatz, dass es auf die Intensität der Werbeschaltungen ankommt sowie darauf, ob die Werbung über mehrere Geräte geschaltet wird und in Form von “Retargeting“ zu einer unzumutbaren Belästigung der betroffenen Person führt. Dies wird beispielsweise nicht der Fall sein, wenn lediglich generische Werbung eines bekannten Online-Modehändlers, die auf einem einfachen demographischen Profil beruht, auf einer Webseite angezeigt wird, oder, wenn Emotionserkennung zur künftigen Anpassung von Produkten und Dienstleistungen eingesetzt wird (Use Case 4.3). Als Beeinträchtigung können hingegen diskriminierende Werbungen, personalisierte Preisangebote oder Werbeanzeigen, die gezielt Schwachstellen von Betroffenen ansprechen und ausnutzen, gesehen werden, wie beispielsweise an spielsüchtige Personen gerichtete Werbeschaltungen für Sportwetten (Use Case 4.1). Für Art 86 AI Act ebenso einschlägig wäre der Einsatz von Emotionserkennung zur Analyse der Kund:innenzufriedenheit, sofern daran eine Entscheidung über die Auflösung des Vertragsverhältnisses geknüpft wird (Use Case 4.3.b). Strittig ist, wie bereits erörtert, ob rein finanzielle Nachteile als Beeinträchtigung gelten, sofern sie nicht ohnehin in Form von rechtlichen Auswirkungen erfasst sind, wobei es auf den Umfang des Nachteils ankommen wird. Werden bspw in Use Case 4.2 Preisanpassungen anhand von Emotionserkennung vorgenommen, so wird im Einzelfall und unter Berücksichtigung der Betroffenenperspektive zu prüfen sein, ob eine ausreichende Beeinträchtigung der finanziellen Gesundheit oder der privaten Lebensführung vorliegt.

Sofern also der Anwendungsbereich des Art 86 AI Act eröffnet ist, steht betroffenen Personen

das Recht zu, eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten. Über dieses Recht muss bereits vorab aufgeklärt werden. Auch im Fall, dass Hochrisiko-KI zur Entscheidungsfindung bzw ein Emotionserkennungssystem eingesetzt wird, muss entsprechend hierüber informiert werden.

### 5.7.3 Zusammenfassende Tabelle zur Einordnung der Fallbeispiele

| | | Use Case 1 | Use Case 2 | Use Case 3 | Use Case 4 | | |
|---|---|---|---|---|---|---|---|
| | | | | | Unterfall 4.1 | Unterfall 4.2 | Unterfälle 4.3.a und 4.3.b |
| DSGVO | **Personenbezogene Daten** | In der Regel ja (im Folgenden wird davon ausgegangen) | | | | | |
| | **„Sensible“ Daten nach Art 9 Abs 1 DSGVO** | Ja | Eher nein | Kommt auf Einzelfall an | Eher nein | Regelmäßig ja | Eher nein |
| | **Abwendungsbereich Art 22 DSGVO** | Ja | Ja, sofern Profiling von einzelnen Personen erfolgt | Ja | Eher ja, sofern automatisierte Entscheidung | Strittig (im Einzelfall zu prüfen) | Unterfall 4.3.a eher nein (keine Beeinträchtigung); Unterfall 4.3.b eher ja |
| | **Art 15 Abs 1 lit h DSGVO** | Ja | Ja, sofern Profiling und somit Art 22 DSGVO erfüllt | Ja | Ja, sofern Art 22 DSGVO erfüllt | Je nachdem, ob Art 22 DSGVO erfüllt | Ja, sofern Art 22 DSGVO erfüllt (4.3.a eher nein; 4.3.b eher ja) |
| | **Informationspflichten nach Art 13 und 14** | Ja | | | | | |

| | | Use Case 1 | Use Case 2 | Use Case 3 | Use Case 4 | | |
|---|---|---|---|---|---|---|---|
| | | | | | Unterfall 4.1 | Unterfall 4.2 | Unterfälle 4.3.a und 4.3.b |
| AI Act | **KI-System** | Regelmäßig ja | | | | | |
| | **Emotionserkennungs-system (EES)** | | | | Im Einzelfall zu prüfen; EES iSd AI Act gegeben, sofern anhand von Gesten emotionale Reaktionen abgeleitet werden | Im Einzelfall zu prüfen; regelmäßig EES iSd AI Act gegeben | Im Einzelfall zu prüfen; EES im Sinne des AI Act bei Unterfall 4.3.b fraglich, bei Unterfall 4.3.a wohl klarer |
| | **Verbotenes System nach Art 5 AI Act** | Nein | Nein | Prinzipiell nein | Ev verbotene Praktik nach Art 5 (1) (b) AI Act | Prinzipiell nein | Prinzipiell nein |
| | **Hochrisiko-KI-System** | Ja | Nein, außer in Kombination mit anderer Hochrisiko-KI | Ja | Ja | Ja | Tendenziell ja; ev Ausnahme gem Art 6 (3) (b) AI Act |
| | **Rechtliche Auswirkung oder ähnliche Beeinträchtigung** | Ja | - | Ja | Ja, insb bei an spielsüchtige Personen gerichteten Werbeschaltungen für Sportwetten | Im Einzelfall zu prüfen, ob Beeinträchtigung vorliegt | Eher nein in Bezug auf 4.3.a. Ja, bei Vertragskündigung in Bezug auf 4.3.b |
| | **Weitere vorab Informationspflichten** | Informationen über Einsatz von Hochrisiko-KI zur Entscheidungsfindung sowie Bestehen eines Rechts nach Art 86 AI Act | | | | | |
| | | | | | Information über Einsatz eines EES an betroffene Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung | | |

# 6 Sozialwissenschaftliche Aspekte

Der sozialwissenschaftliche Blick auf das Auskunftsrecht und die damit verbundenen Herausforderungen erweitert die Perspektive über die bisher dargestellten rechtlichen Aspekte hinaus. Diese Sichtweise ist besonders wichtig, da sie aufzeigt, warum dem Auskunftsanspruch in der Praxis mitunter nicht entsprochen wird. Daraus lassen sich wiederum Rückschlüsse auf Art 86 AI Act und dessen praktische Umsetzbarkeit ziehen. Eng damit verknüpft ist das bereits erwähnte Phänomen des sogenannten „Automation Bias“: Personen, die in KI-gestützte Entscheidungen eingebunden sind, neigen häufig dazu, sich übermäßig auf automatisierte Systeme zu verlassen, ohne deren Ergebnisse kritisch zu hinterfragen. Auch daraus ergeben sich wichtige Erkenntnisse für die Praxis und Hinweise auf notwendige Maßnahmen.

## 6.1 Auskunft

Unsere Recherchen zeigen, dass der datenschutzrechtliche Anspruch auf Auskunft in jüngster Vergangenheit wiederholt Gegenstand empirischer Untersuchungen war. Aus der Metaanalyse von *Habu & Henderson* (2023) geht bspw hervor, dass die Forschungsaktivitäten dazu seit 2013 deutlich angestiegen sind und das Auskunftsrecht offenbar auch das am meisten beforschte Betroffenenrecht ist.[386]

Das Recht auf Auskunft gilt allgemein als „zentrales Betroffenenrecht“.[387] Seine besondere Stellung erhält der Rechtsanspruch aus juristischer Sicht zunächst dadurch, dass dieser auch auf verfassungsrechtlicher Ebene über Art 8 Abs 2 der GRC ausdrücklich gewährleistet ist.[388] In teleologischer Hinsicht besteht die Bedeutung (bzw der Zweck) des Anspruchs vor allem darin, dass dieser in vielen Fällen erst die Geltendmachung weiterer Betroffenenrechte (wie zB das Recht auf Berichtigung gem Art 16 DSGVO, das Recht auf Löschung gem Art 17 DSGVO oder das Recht auf Widerspruch gem Art 21 DSGVO) möglich macht. So dient das Recht auf Auskunft auch dazu, automationsunterstützte Entscheidungsprozesse oder unrechtmäßige Datenverarbeitungspraktiken überhaupt erst offenzulegen bzw festzustellen.

Im Rahmen des europäischen Forschungsprojekts IRISS (Increasing Resilience in Surveillance Societies)[389] wurde unter der Leitung des britischen Kriminologen *Clive Norris* von 2012 bis 2015 eine systematische Untersuchung zur praktischen Ausübung und Durchsetzung des Auskunftsrechts durchgeführt.[390] Die Studie deckt insgesamt zehn

[386] *Habu/Tristan*, Data subject rights as a research methodology, Journal of Responsible Technology 2023, 100070.
[387] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG[2] Art 15 DSGVO 419.
[388] *Bäcker* in *Kühling/Buchner,* Datenschutz-Grundverordnung[2] Art 15 DSGVO 419.
[389] *European Commission*, Increasing Resilience in Surveillance Societies, https://cordis.europa.eu/project/id/290492/reporting (abgerufen am 14. 2. 2025).
[390] *Norris/L'Hoiry/Galetta/Hert/Szekely/Raab*, Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform, https://www.statewatch.org/media/documents/news/2015/feb/iriss-policy-brief.pdf (Stand 31. 1. 2015).

europäische Länder ab,[391] wobei über 300 öffentliche und private Organisationen und 184 Antworten auf Auskunftsbegehren eingehend untersucht wurden. Dabei wird im Hinblick auf Auskünfte über automatisierte Entscheidungsfindungsprozesse berichtet, dass diese in mehr als zwei Drittel der Fälle (71 %) entweder gar nicht oder nicht in rechtskonformer Weise erteilt wurden. Weiters mussten mehr als ein Fünftel (21 %) aller Fälle der Stichprobe aufgrund des Verhaltens der datenschutzrechtlich Verantwortlichen an die jeweiligen nationalen Datenschutzbehörden weitergeleitet werden.[392]

Mit konkretem Bezug auf Österreich lässt sich weiters auf eine qualitative Studie von *Rothmann* (2017) zu Datenverarbeitungen über Videoüberwachung verwiesen.[393] Dabei wurden in den Jahren 2013 und 2014 insgesamt 29 Auskunftsanfragen an unterschiedliche Betreiber derartiger Systeme gestellt und deren Reaktionen bzw Antwortverhalten analysiert. Die Studie legt offen, mit welchen Strategien die Verantwortlichen die Anfragen zurückweisen und den Anspruch auf Auskunft verweigern. Dazu zählen bspw die fehlende Offenlegung von Kontaktdaten oder Ansprechpersonen, wodurch es erschwert wird, überhaupt eine Anfrage zu stellen, ebenso wie Formen der Zurückweisung und Verneinung des rechtlichen Anspruchs oder Verweise auf strittige Auslegungen des Datenschutzrechts, wonach die Betroffenen bspw für die Auskunft ein Leumundszeugnis vorlegen müssten oder die Auskunft selbst wiederum die Rechte Dritter verletzen würde und daher nicht erteilt werden könne.[394] Im Ergebnis haben die Verantwortlichen der Überwachungssysteme nur in sechs Fällen, wie gesetzlich vorgesehen, auch das Videomaterial beauskunftet, wobei nur in zwei Fällen eine vollständige Datenübermittlung stattfand. In lediglich 14 von 29 Anfragen wurden auch die zugehörigen rechtlichen Informationen (wie zB zum Verwendungszweck, zur Rechtsgrundlage, oder zu den Empfängern der Daten) beauskunftet, wobei dies ebenfalls nur in drei Fällen auch im gesetzlich erforderlichen Umfang erfolgte.[395] Die empirischen Ergebnisse in diesem Bereich werden als stark situationsbezogen bezeichnet, es zeigt sich jedoch insgesamt wiederholt, dass die Verantwortlichen dazu tendieren, dem gesetzlichen Anspruch nur begrenzt Folge zu leisten und sich häufig der Rechenschaftspflicht zu entziehen versuchen.[396]

Zudem kann in diesem Zusammenhang auch auf die Studie von *Wulf & Seizov* (2024) verwiesen werden.[397] Mit Bezugnahme auf Art 15 und Art 22 der DSGVO haben diese ebenfalls die Effektivität des Auskunftsrechts untersucht. Dazu wurde zunächst ein Online-Survey (n=835) mit Bezug auf britische Konsument:innen durchgeführt, um herauszufinden,

---

[391] Diese Untersuchung wurde in den folgenden Ländern durchgeführt: Österreich, Belgien, Deutschland, Ungarn, Italien, Luxemburg, Norwegen, Slowakei, Spanien und Großbritannien.
[392] *Norris/L'Hoiry*, Exercising Citizen Rights Under Surveillance Regimes in Europe. Meta-analysis of a Ten Country Study, in *Norris/Hert/L'Hoiry/Galetta* (Hrsg), The Unaccountable State of Surveillance. Law, Governance and Technology Series (2017) 405.
[393] *Rothmann,* Video Surveillance and the Right of Access. The empirical proof of panoptical asymmetries, Surveillance & Society 2017, 222; siehe auch *Rothmann*, Videoüberwachung und Auskunftsrecht. Eine empirische Analyse visueller Ansprüche, DuD 2014, 405.
[394] Siehe hierzu auch DSB 12. 5. 2008, K121.385/0007-DSK/2008; 30. 7. 2010, K121.605/0014-DSK/2010; 7. 9. 2013, K121.698/0004-DSB/2013; 9. 6. 2013, K121.605/0003-DSK/2013.
[395] Von ähnlichen Erfahrungen im Fall von Videoüberwachung berichtet auch die britische Studie *Spiller,* Experiences of accessing CCTV data. The urban topologies of subject access requests, Urban Studies 2016, 2885.
[396] *Habu/Tristan*, Journal of Responsible Technology 2023, 100070.
[397] *Wulf/Seizov*, „Please understand we cannot provide further information". Evaluating content and transparency of GDPR-mandated AI disclosures, AI & Society 2024, 235 (235 ff).

welche subjektiven Erwartungen die Betroffenen von der Auskunft über automationsunterstütze Datenverarbeitungsprozesse und KI-basierte Einzelentscheidungen haben.[398] Dabei zeigt sich, dass etwa die Hälfte der Befragten weder weiß, ob sie jemals einen KI-basierten Dienst genutzt haben (51%), noch ob sie jemals einer automatisierten Einzelentscheidung ausgesetzt waren (56%). Weiters zeigt der Survey, dass rund 44% der Befragten sowohl über die eigentliche Verwendung eines KI-basierten Algorithmus als auch über die dahinterliegende Logik und die dabei verarbeiteten personenbezogenen Daten informiert werden möchten. Weitere 15% gehen noch einen Schritt weiter und möchten, dass der „Computer Code“ hinter dem Algorithmus offengelegt wird.

Darüber hinaus wurden – ähnlich wie in den oben genannten Studien – insgesamt 100 Auskunftsanfragen an verschiedene Unternehmen bzw Organisationen gestellt und deren Rückmeldungen systematisch ausgewertet. Anders als bei der Online-Survey beziehen sich die Auskunftsanfragen auf deutsche Unternehmen, wobei eine heterogene Auswahl von Sektoren getroffen wurde, welche von „Airline“ und „Carsharing“ über „Insurance“ bis hin zu „Utility“ reichen.[399]

Die nachfolgende Tabelle zeigt die Auswertung der formalen Kriterien. Demnach hatten die Unternehmen in etwas mehr als der Hälfte der Fälle einen speziellen und deutlich gekennzeichneten Kommunikationskanal für Datenschutzanfragen, über den es einfach war die Anfragen zu stellen. Die Zeit zur Beantwortung der Auskunftsanfragen beträgt im Schnitt rund 3 Wochen. Der Umfang der textbasierten Auskunft bewegt sich zwischen einem Minimum von 29 und einem Maximum von über 19.000 Wörtern. Weiters zeigt die Auswertung bspw, dass rund 32% der Unternehmen in ihrer Auskunft lediglich auf die Datenschutzerklärung verweisen.

Neben der Auswertung formaler Kriterien erfolgte zudem eine linguistische Analyse der textbasierten Antworten. Dabei zeigt sich, dass lediglich die Hälfte der Antworten auch in sprachlicher Hinsicht als transparent bezeichnet werden können, also weitgehend frei von verworrenen Sätzen, übermäßigem Rechts- bzw Fachjargon oder modalen Formulierungen sind, die den Umfang, die Art und die Häufigkeit der automatisierten Datenverarbeitung, die die Organisation vornimmt, verschleiern.

Laut den gemachten Angaben nutzen rund 66% der Unternehmen die eine oder andere Form KI-basierter Datenverarbeitung. Die meisten Unternehmen nutzen KI zur Verbesserung der „customer experience“ und zur Optimierung von Produkt- und Serviceangeboten. Mit 30 bzw 26 %, sind Formen des Profilings und der automatisierten Entscheidungsfindung die am wenigsten verbreiteten KI-Anwendungen. Die Autoren gehen in ihrer Analyse jedoch auch davon aus, dass die angefragten Unternehmen wiederholt falsche Angaben machen bzw schlicht nicht angeben, dass sie KI-basierte Verfahren der Datenverarbeitung nutzen.

[398] Die Stichprobe bezieht sich laut den Autoren auf britische Respondenten und wird als explorativ (dh nicht repräsentativ) bezeichnet; siehe *Wulf/Seizov*, AI & Society 2024, 235 (238).
[399] *Wulf/Seizov*, AI & Society 2024, 235 (241).

Tabelle: Formale Kriterien in der Beantwortung von Auskunftsanfragen (explorative Stichproben von n=100 Unternehmen bzw Organisationen)

| | | | | | |
|---|---|---|---|---|---|
| **Means of First Contact** | **Email**<br>81% | **Contact Form**<br>18% | **Other**<br>1% | | |
| **Ease of First Contact** | **Easy**<br>54% | **Neutral**<br>43% | **Difficult**<br>3% | | |
| **Reply Time (Days)** | **Min**<br>1 | **Median**<br>12 | **Mean**<br>23 | **Max**<br>112 | **S.D.**<br>28.56 |
| **Length of Personalised Reply (Words)** | 20 | 272 | 654.80 | 11,977 | 1,470.37 |
| **Length of Disclosure (Response + Add-ons, Words)** | 29 | 1,260 | 2,379.48 | 19,116 | 3,046.39 |
| **Medium of AI Response** | **Plain Email**<br>60% | **Secure Email**<br>3% | **Account Area**<br>9% | **Webpage**<br>4% | **Regular Mail**<br>24% |
| **Number of Messages Exchanged** | **1**<br>64% | **2 - 3**<br>21% | **4 - 5**<br>9% | **6 - 7**<br>5% | **8**<br>1% |
| **Additional Authentication Requested** | **None**<br>88% | **Picture ID**<br>7% | **Account Data**<br>4% | **Multiple**<br>1% | |
| **Contact Person's Role** | **Customer Service**<br>37% | **Privacy Officer**<br>31% | **Legal Counsel**<br>8% | **Unknown / Other**<br>24% | |
| **Degree of Response Personalization** | **Privacy Policy Reference**<br>32% | **Generic GDPR Response**<br>22% | **Personalized Response**<br>46% | | |
| **Personal Data Enclosed** | **None**<br>65% | **General GDPR Data**<br>11% | **AI-Processed Data**<br>24% | | |

Zusammenfassend stellen die Autoren fest, dass die Angaben zu KI-basierten Anwendungen und automatisierten Datenverarbeitungen in 51 % der Fälle entweder „opaque“ sind bzw nicht vollständig auf die Thematik eingegangen wird. Anstatt offenzulegen, welche Algorithmen eingesetzt werden, wie sie funktionieren und zu welchem Zweck, verschleiern viele Unternehmen diese Informationen durch irreführende oder überfrachtete Formulierungen. Nur 18 % der Angaben werden als hinreichend bestimmt und transparent bezeichnet.

## 6.2 Automation Bias

Digitale Systeme operieren grundsätzlich auf Basis binärer Codes (O/1). Der Entstehungsprozess des Codes zur Datenverarbeitung und Analyse verschiedener Szenarien ist in einen spezifischen soziokulturellen Kontext eingebettet.[400] KI-basierte Entscheidungsfindungssysteme arbeiten niemals völlig objektiv; die Kriterien und Schwellenwerte zur Beurteilung, wann etwas als richtig oder falsch, verdächtig oder unverdächtig, relevant oder irrelevant klassifiziert wird, unterliegen verschiedenen (methodischen) Ansätzen, Sichtweisen und Wertigkeiten, die gewissermaßen in die Software eingeschrieben sind und sich im Code manifestieren.[401]

Zudem bauen algorithmische Entscheidungssysteme auf Prämissen der statistischen Wahrscheinlichkeit auf, weshalb bestimmte Entscheidungen per se einem gewissen Signifikanz- bzw Fehlerniveau (wie zum Beispiel $\alpha = \leq 5\%$ oder $\leq 1\%$) unterliegen. Dies bedeutet letztlich, dass keine Bewertung bzw Klassifizierung des Systems als eindeutiger Treffer verstanden werden kann. Es handelt sich vielmehr um einen von Menschen festgelegten Schwellenwert probabilistischer Einstimmung.[402] Wird dieser Schwellenwert zu hoch angesetzt, besteht die Gefahr, ein sicherheitskritisches Szenario nicht zu erkennen (false rejection); wird das System sensibel eingestellt, impliziert dies wiederum eine vermehrte Zahl an Fehlalarmen (false acceptance).[403]

Der Verweis auf derartige methodische Unzulänglichkeiten und mögliche Verzerrungen ist deshalb relevant, weil davon ausgegangen wird, dass Menschen dazu tendieren, die Informationen und Entscheidungen eines computerbasierten Systems jenen natürlicher Personen gleichzustellen oder diesen sogar vorzuziehen.[404] Frühe Studien zu diesem Phänomen finden sich insb in der Luftfahrt- und Cockpitforschung unter dem Begriff „Complacency“.[405] Das US-amerikanische National Aeronautics and Space Administration

[400] Siehe weiterführend auch die Ausführungen des ErwG 44 AI Act.
[401] *Bowker/Star*, Sorting Things Out. Classification and Its Consequences (2000); *Graham/Wood*, Digitizing Surveillance. Categorization, Space, Inequality, Critical Social Policy 2003, 227 (231 ff); *Rothmann/Vogtenhuber,* Abweichendes Verhalten und automationsunterstützte soziale Kontrolle, Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (288 ff).
[402] *Rothmann/Vogtenhuber,* Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (288 ff).
[403] *Introna/Wood*, Picturing Algorithmic Surveillance. The Politics of Facial Recognition Systems, Surveillance & Society 2004, 188; *Kammerer*, Bilder der Überwachung (2008) 202 ff.
[404] *Reeves/Nass*, The media equation. How people treat computers, television, and new media like real people and places (2002); *Rothmann/Vogtenhuber,* Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (288 ff).
[405] *Parasuraman/Manzey*, Complacency and Bias in Human Use of Automation, Human Factors 2010, 381; *Wiener* beschreibt diesen als “psychological state characterized by a low index of suspicion“, *Wiener,* Complacency. Is the

Center definiert den Begriff als „self-satisfaction that may result in non-vigilance based on an unjustified assumption of satisfactory system state".[406] Erste empirische Nachweise dieses Effekts wurden über verschiedene experimentelle Versuchsanordnungen bereits Anfang der 1990er Jahre erbracht.[407]

In jüngster Zeit wurde dieses sozio-technische Problem auch unter dem Begriff des sog „automation bias" diskutiert.[408] Darunter wird allgemein die Tendenz verstanden, sich in bestimmten Situationen übermäßig auf automationsunterstützte Entscheidungsfindungssysteme zu verlassen, ohne deren Output kritisch zu prüfen.[409] Demnach werden automationsunterstützte Entscheidungen oder Empfehlungen im praktischen Einsatz eher für gültig und berechtigt gehalten, wenngleich diese möglicherweise falsche oder unvollständige Informationen liefern.[410]

Das Phänomen des Automation Bias hat vor allem im Bereich der Medizin vermehrte Aufmerksamkeit erfahren.[411] So bspw im Zusammenhang mit KI-gestützter Mammographie, wo der Bias ebenso zu falschen Brustkrebsdiagnosen wie zu unnötigen Biopsien bei Personen ohne Anomalien führen kann.[412] In einer Studie von *Khera et al* (2023) wird bspw berichtet, dass das medizinische Personal das automatisierte Entscheidungsfindungssystem sogar in kontrollierten Umgebungen ohne Zeitdruck bevorzugten und sich auf das KI-basierte Tool verließen, obwohl widersprüchliche oder klinisch unsinnige Informationen vorlagen.[413]

In einer britischen Studie von *Goddard et al* (2012) mit dem Titel „Automation bias: a systematic review of frequency, effect mediators, and mitigators" wurden insgesamt 74 internationale (medizinische) Beiträge einer Metaanalyse unterzogen.[414] Im Zuge dessen werden verschiedene Faktoren beschrieben, die den Automation Bias beeinflussen bzw begünstigen können. Als userseitige Einflussfaktoren identifizieren die Autor:innen dabei kognitive Eigenheiten der Nutzer:innen ebenso wie aufgabenspezifische Vorerfahrungen, Einstellungen (wie Vertrauen bzw Zuversicht) und Überzeugung. Umweltseitig werden Faktoren wie Arbeitsbelastung, Aufgabenkomplexität sowie Zeitdruck genannt, welche ebenfalls wiederum kognitive Auswirkungen haben können.[415] In der Forschung wird zudem

term useful for air safety? in Flight Safety Foundation (Hrsg), Proceedings of the 26th Corporate Aviation Safety Seminar. Denver, CO 1981 (1981) 116.

[406] *Billings/Lauber/Funkhouser/Lyman/Huff*, Aviation Safety Reporting System (1976) 23.

[407] *Parasuraman/Manzey*, Human Factors 2010, 381 (383 ff).

[408] *Alon-Barkat/Busuioc*, Human–AI Interactions in Public Sector Decision Making. "Automation Bias" and "Selective Adherence" to Algorithmic Advice, Journal of Public Administration Research and Theory 2023, 153; *Logg*, Algorithm Appreciation. People Prefer Algorithmic to Human Judgment, Organizational Behavior and Human Decision Processes 2019, 90.

[409] *Wickens/Clegg/Vieane/Sebok*, Complacency and Automation Bias in the Use of Imperfect Automation, Human Factors 2015, 729.

[410] Dies impliziert auch, dass KI-basierte Entscheidungen tendenziell weniger verhandelbar werden. Der Code wird somit im Sinne Lessig's zum Gesetz (Code is Law) und der Algorithmus zur normsetzenden Kraft im Sozialen. *Lessig,* Code – Version 2.0 (2006); vgl auch *Kammerer*, Bilder der Überwachung 205; *Rothmann/Vogtenhuber*, Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (289).

[411] *Goddard/Roudsari/Wyatt*, Automation bias. A systematic review of frequency, effect mediators, and mitigators, J AmMed Inform Assoc 2012, 121.

[412] *Baltzer*, Automation Bias in Breast AI, Radiology 2023, e230770.

[413] *Khera/Simon/Ross*, Automation Bias and Assistive AI, Risk of Harm From AI-Driven Clinical Decision Support, jama 2023, 2255.

[414] *Goddard/Roudsari/Wyatt*, J AmMed Inform Assoc 2012, 121 (121 ff).

[415] *Goddard/Roudsari/Wyatt*, J AmMed Inform Assoc 2012, 121 (121 ff).

davon berichtet, dass Nutzer:innen mit geringerer Erfahrung eher dazu tendieren, KI-Systemen gegenüber abgeneigt zu sein, wohingegen die Voreingenommenheit gegenüber der Automatisierung mit höherem Wissensstand abnimmt.[416]

Als Strategie zur Abschwächung des Automation Bias wird in der Literatur wiederholt die Möglichkeit von Schulungen oder verschiedenen Formen unterstützender Informationsbereitstellung thematisiert. Diese Informationen und gestalterische Faktoren wie die Position der Ratschläge auf dem Bildschirm und die Art der Beratung (zB Information vs Empfehlung) können demnach die Entscheidungsfindung verbessern.[417] Die deutsche Studie von *Bahner et al* (2008) hat hierzu untersucht, welchen Effekt spezifische Trainings bzw Schulungen auf den Umgang mit automatisierten Entscheidungen und einem möglicherweise damit verbundenen Automation Bias haben.[418] So wurde festgestellt, dass dadurch die Nachlässigkeit bzw Gleichgültigkeit der Nutzer:innen gegenüber möglicherweise verzerrten Ergebnissen reduziert wird, dh die Nutzer:innen die automatisierten Entscheidungen also eher hinterfragen. Schulungen können demnach ein geeignetes Mittel zur Verringerung des Risikos darstellen, sich von einem vermeintlichen Bias täuschen zu lassen, wenngleich sich dieses Risiko letztlich auch damit nicht vollständig vermeiden lässt.

Die australische Studie von *Vereda et al* (2023) zeigt wiederum, wie die Bereitstellung allgemeiner Erläuterungen zur Funktionsweise sogenannter „Intelligent Agents“ den Automation Bias beeinflusst. Demnach wird der Bias dadurch nicht unbedingt verringert, sondern manchmal sogar verstärkt.[419] Informationen bzw Erläuterungen können jedoch die menschliche Entscheidungszeit verkürzen und die Entscheidungsgenauigkeit der Nutzer:innen erhöhen. Insgesamt sei der Ansatz zwar wirksam, die Vorteile gelten allerdings als stark kontextabhängig. Schließlich wird in der Debatte auch ein Zielkonflikt (trade-off) zwischen dem Grad der Voreingenommenheit der Nutzer:innen und der Genauigkeit des Systems thematisiert. Dabei sei eine Balance anzustreben, wobei den Nutzer:innen einerseits geholfen werden soll, Entscheidungen besonders genauer und robuster Systeme zu akzeptieren, also „algorithmic aversion“ zu reduzieren, in bestimmten Situationen jedoch zugleich skeptisch zu bleiben.[420]

In Anlehnung an *Baltzer* (2023) lassen sich zur Abschwächung der Auswirkungen von Automatisierungsverzerrungen für die organisationsseitige Implementierung die Umsetzung der folgenden Strategien empfehlen:[421]

- **Schulung und** kontinuierliche **Sensibilisierung** (Weiterbildung) für Nutzer:innen von automatisierten Systemen, um das Bewusstsein für das Problem des Automation Bias zu schärfen und die Fähigkeit zu fördern, fundiertere Entscheidungen zu treffen, automatisierungsbedingte Nachlässigkeit zu vermeiden und automatisierte

[416] *Horowitz/Kahn*, Bending the Automation Bias Curve. A Study of Human and AI-Based Decision Making in National Security Contexts, International Studies Quarterly 2024, sqae020.
[417] *Goddard/Roudsari/Wyatt*, J AmMed Inform Assoc 2012, 121 (125).
[418] *Bahner/Hüper/Manzey*, Misuse of automated decision aids. Complacency, automation bias and the impact of training experience, Int. J. Human-Computer Studies 2008, 688.
[419] *Vereda/Livnia/Douglas/Howeb/Millerc/Sonenberg*, The effects of explanations on automation bias, Artificial Intelligence 2023, 103952.
[420] *Vereda et al*, Artificial Intelligence 2023, 103952.
[421] *Baltzer*, Radiology 2023, e230770.

Entscheidungen kritisch zu hinterfragen.

- **Design** und **Entwicklung** eines **transparenten Systems**, das die eigenen Unsicherheiten anzeigt bzw kommuniziert und den Nutzer:innen so hilft, die Zuverlässigkeit der automatisierten Empfehlungen besser einzuschätzen. Dies impliziert die regelmäßige technische Validierung und Sicherstellung von Akkuratheit und Robustheit des Systems.
- Allgemein geht es zudem um eine **Sicherstellung der Verantwortlichkeit** für die Entscheidungen und Identifikation bzw Ausweisung entsprechender Ansprechpersonen.

# 7 Ethische Aspekte

Neben rechtlichen und sozialwissenschaftlichen Aspekten wohnt dem Recht auf Erklärung und dem generellen Umgang mit KI-basierten Systemen auch eine starke ethische Komponente inne. Ethik wird im Allgemeinen als philosophische Reflexion über moralische Konzepte, wie bspw „gut“ und „böse“ oder „richtig“ und „falsch“, definiert[422] und hat als philosophische Disziplin die kritische Untersuchung normativer Annahmen, Werte und Urteile, die der Entscheidungsfindung und dem Handeln zugrunde liegen, zum Gegenstand.[423] Ein Ethikverständnis, das die Lebenswirklichkeit und ihre spezifischen Probleme widerspiegelt, wird häufig mit der ethischen Subdisziplin der Angewandten Ethik in Verbindung gebracht, deren Ziel es ist, Fragen zu analysieren, die sich in bestimmten Bereichen stellen, etwa in der Bioethik, der Technikethik, der Wirtschaftsethik, der Rechtsethik oder der politischen Ethik.[424] Ein Feld der Angewandten Ethik und Unterdisziplin der Technikethik ist die sogenannte „KI-Ethik“, welche sich mit normativen Fragen, die durch die Konzeption, Entwicklung, Implementierung und Nutzung von KI aufgeworfen werden, auseinandersetzt.[425]

Die Entwicklung der KI-Ethik verdeutlicht die signifikanten ethischen Implikationen Künstlicher Intelligenz für den Menschen und die Gesellschaft im Allgemeinen, welche sich mittlerweile auf beinahe all unsere Lebensbereiche erstrecken.[426] Diese Implikationen umfassen die sich wandelnde Beziehung zwischen Menschen und Maschinen und werfen wesentliche Fragen hinsichtlich menschlicher Autonomie, Würde, Fairness, Transparenz sowie der weitergehenden gesellschaftlichen und ökologischen Auswirkungen von KI auf.[427] Zusammengefasst manifestiert sich dabei dieser sogenannte „ethische Impact“ von Künstlicher Intelligenz „in sowohl ethischen Risiken als auch in ethischen *Benefits*, die durch den Einsatz von entweder bestimmten KI-Systemen selbst, von KI in bestimmten Sektoren, gegenüber bestimmten Personen(-gruppen) oder in gewissen Kontexten entstehen können.“[428] Diese Auswirkungen, wozu beispielsweise Fragen des gesellschaftlichen Wohlergehens, der sozialen Inklusion oder des demokratischen Diskurses zählen, finden in den bestehenden rechtlichen Rahmenbedingungen jedoch nur unzureichend Berücksichtigung.[429]

Als Antwort auf die mit dem zunehmenden technologischen Fortschritt in der KI-Forschung einhergehenden Herausforderungen haben zahlreiche Organisationen ethische Leitlinien entwickelt, die als Standard oder Orientierung für die Entwicklung und den Einsatz von KI

[422] Siehe die Definition in: *Singer,* Ethics. philosophy, https://www.britannica.com/topic/ethics-philosophy (Stand 13. 2. 2025).
[423] *Rubeis,* Ethics of Medical AI (2024) 56.
[424] Vgl *Pauer-Studer*, Einführung in die Ethik[3] (2020) 14.
[425] Vgl *Stahl,* From computer ethics and the ethics of AI towards an ethics of digital ecosystems, AI and Ethics 2022, 65 und *AI HLEG,* Ethik-Leitlinien 37.
[426] Vgl *Mantelero,* Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI (2022) 93.
[427] Vgl *Mantelero,* Beyond Data 93.
[428] *Poindl/Scheichenbauer/Müller*, Folgenabschätzungs-Methodologie. Datenschutz, Grundrechte, Ethik, in *Eisenberger/Klaushofer* (Hrsg), KI-VO. Exekutive Rechtsetzung, Standardisierung, Zertifizierung und Grundrechte-Folgenabschätzung (2025) iE.
[429] Vgl *Poindl/Scheichenbauer/Müller* in *Eisenberger/Klaushofer* iE.

dienen sollen. Als Beispiele können die Ethik-Leitlinien für eine vertrauenswürdige KI der Unabhängigen Hochrangigen Expertengruppe für Künstliche Intelligenz[430] zusammen mit der darauf aufbauenden Bewertungsliste „ALTAI"[431], die KI-Grundsätze der OECD[432] sowie die UNESCO-Empfehlungen zur Ethik der Künstlichen Intelligenz[433] angeführt werden. Diese Dokumente fordern den Einsatz vertrauenswürdiger KI und beruhen auf der Wahrung der Menschenwürde und der Autonomie.

Die Prinzipien der Transparenz und Erklärbarkeit von KI-gestützten Prozessen nehmen einen besonders hohen Stellenwert in all diesen Leitfäden ein, aber auch andere in diesen Dokumenten angeführte Prinzipien, wie etwa das Prinzip der Verantwortlichkeit, der menschlichen Aufsicht, der Nicht-Diskriminierung, der Effizienz oder des Vertrauens, sind für das Recht auf Erklärung von Bedeutung. An dieser Stelle ist insb auf die Metastudie von Jobin et al (2019) zur „Global landscape of AI ethics guidelines" zu verweisen, in welcher ein Überblick über den bestehenden Korpus von Dokumenten gegeben wird, die von Organisationen herausgegebene Soft-Law-Normen oder ethische Leitlinien zum Einsatz von KI enthalten. Darin wird ebenfalls untersucht, welche Aussagen sich aus den genannten Prinzipien für das Recht auf Erklärung ableiten lassen und welche Informationen über KI-Systeme in diesem Sinne offengelegt werden sollten. Die meisten Quellen nannten dabei generelle Erläuterungen zum Einsatz des Systems, den Quellcode, die Datenverwendung, potenzielle Auswirkungen und Erklärungen in nicht-technischer Sprache als wichtige Erfordernisse.[434]

Diese Erfordernisse und folgende weitere Elemente (siehe sogleich die Punkte 1-10) können in Rekurs auf ethische Leitfäden und Publikationen als wesentliche Inhalte des Rechts auf Erklärung aus ethischer Perspektive ausgemacht werden. Es ist darauf hinzuweisen, dass sich diese Elemente nicht ausschließlich auf einzelfallbezogene *ex post*-Erklärungen beziehen, sondern einige auch auf allgemeine *ex ante*-Erklärungen abzielen, damit für betroffene Personen bereits im Vorhinein ersichtlich ist, wie das System operiert. Denn in Bezug auf Erklärungen lassen sich im Allgemeinen jene zur generellen Funktionalität des KI-Systems (Modellerklärbarkeit oder globale Erklärbarkeit), die sowohl im Vorhinein als auch im Nachhinein möglich sind, und jene zu Einzelentscheidungen (lokale Erklärbarkeit oder Datenerklärbarkeit) unterscheiden[435], wobei im Folgenden beide Erklärungsansätze miteinbezogen werden:

1. **Erklärung des Entscheidungsprozesses:** Eine Erklärung, ob und wie Algorithmen eine Entscheidung getroffen haben und mit welcher Begründung welche Modelle und Methoden eingesetzt wurden. Darunter fällt auch eine Begründung, weshalb die

[430] *AI HLEG,* Ethik-Leitlinien 2019.
[431] *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment (2020), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342.
[432] *OECD,* AI principles, https://oecd.ai/en/ai-principles (abgerufen am 14. 2. 2025).
[433] *UNESCO,* Recommendation on the Ethics of Artificial Intelligence (2022), https://unesdoc.unesco.org/ark:/48223/pf0000381137.
[434] *Jobin/Ienca/Vayena,* The global landscape of AI ethics guidelines, nature machine intelligence 2019, 389 (391).
[435] Vgl *Deutsches Bundesministerium für Arbeit und Soziales (BMAS)*, Selbstverpflichtende Leitlinien für den KI-Einsatz in der behördlichen Praxis der Arbeit und Sozialverwaltung (2022) 56, https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/a862-01-leitlinien-ki-einsatz-behoerdliche-praxis-arbeits-sozialverwaltung.pdf?__blob=publicationFile&v=2 sowie die näheren Ausführungen in Abschnitt 5.4.2.

spezifische Entscheidung unter mehreren etwaigen alternativen Entscheidungsmöglichkeiten ausgewählt wurde.[436]

2. **Transparenz der verwendeten Daten:** Dies beinhaltet eine detaillierte Auflistung der Eingabedaten, ihrer Herkunft sowie Informationen darüber, wie die Daten verarbeitet werden.[437]
3. **Transparenz der verwendeten Modelle und Algorithmen:** Informationen über die Funktionsweise der verwendeten Modelle (bspw Entscheidungsbäume oder tiefe neuronale Netze) sowie deren potenzielle Fehlerquellen.[438]
4. **Einfluss wesentlicher Merkmale** auf die Entscheidung und Analyse der Gewichtung dieser Merkmale. Dies soll auch zur Fairness beitragen und etwaige Diskriminierungen oder „Bias“ aufzeigen.[439]
5. **Verständlichkeit und Nachvollziehbarkeit der Erklärung:** Erklärungen müssen in klarer, nicht-technischer und verständlicher Sprache verfasst werden und derart an die Expertise der betroffenen Person angepasst werden, dass diese die Erklärung nachvollziehen kann.[440]
6. **Beteiligung menschlicher Aufsicht:** Die Erklärung sollte auch Informationen darüber beinhalten, inwieweit und in welchem Umfang menschliche Entscheidungsträger:innen in die Entscheidungsfindung einbezogen sind.[441]
7. **Rechtsgrundlage der Entscheidung:** Die rechtliche Grundlage der Entscheidung sollte transparent gemacht werden. Dies beinhaltet auch, Anfechtungsmöglichkeit der Entscheidung offenzulegen und Betroffene über ihre Rechte zu informieren.[442]
8. **Auswirkungen der Entscheidung:** Es ist anzuraten, die potenziellen Auswirkungen der Entscheidung auf die betroffene Person darzulegen, welche ebenso den sozialen und wirtschaftlichen Kontext beinhalten soll.[443]
9. **Verantwortlichkeit und Haftung:** Verantwortliche Personen sollten generell sowie gegenüber den Betroffenen klar benannt werden, um eine klare Zuordnung bei Fehlentscheidungen zu ermöglichen und Betroffene darüber zu informieren, an wen sie sich wenden können.[444]
10. **Ethik der Entscheidungsfindung:** Ethische Überlegungen sollten von Anfang an in

[436] Vgl *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 14; *AI HLEG,* Ethik-Leitlinien für eine vertrauenswürdige KI 18; *OECD,* AI principles; *Deutsches Bundesministerium für Arbeit und Soziales*, Selbstverpflichtende Leitlinien für den KI-Einsatz 55.
[437] Vgl *OECD,* AI principles; *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22; *Deutsches Bundesministerium für Arbeit und Soziales*, Selbstverpflichtende Leitlinien für den KI-Einsatz 55; *Brey/Dainow*, AI and Ethics 2024, 1265 (1269).
[438] Vgl *AI HLEG,* Ethik-Leitlinien für eine vertrauenswürdige 18; *OECD,* AI principles.
[439] Vgl *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 16; *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22.
[440] Vgl *AI HLEG,* Ethik-Leitlinien für eine vertrauenswürdige KI 18; *OECD,* AI principles; *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22.
[441] Vgl *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 8.
[442] Vgl *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22.
[443] Vgl *OECD,* AI principles.
[444] Vgl *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 21.

die Entwicklung und das Design von KI-Systemen mit einfließen („Ethics-by-Design“).[445] Jene ethischen Überlegungen, die der Entscheidung zugrunde liegen, sollten transparent gemacht werden, um das Vertrauen in die moralische Integrität des Systems zu stärken.[446]

[445] Vgl *AI HLEG,* Ethik-Leitlinien für eine vertrauenswürdige KI 21.
[446] Vgl *Brey/Dainow*, AI and Ethics 2024, 1265 (1267ff).

# 8 Conclusio

Es kann festgehalten werden, dass das Recht auf Erklärung im Zeitalter zunehmender KI-gestützter Entscheidungsfindungen vor neue Herausforderungen gestellt wird. Damit verbundene Unsicherheiten und offene Rechtsfragen gilt es jedoch zu klären, da das Recht auf Erklärung als essenzielles Betroffenenrecht dazu dient, Entscheidungen überprüfbar zu machen und Betroffenen ein Werkzeug bietet, damit verbundene Folgerechte durchzusetzen. Der gegenständliche Grundlagenbericht hat aufgezeigt, dass die gemeinsame und dennoch abgegrenzte Betrachtung der datenschutzrechtlichen Aspekte einerseits und der neuen Regelung des Art 86 AI Act andererseits zwingend ist und zugleich dazu führt, dass trotz notwendigerweise mangelnder Praxis mit dem AI Act viele Fragen bereits durch die Judikatur zum Datenschutz beantwortet werden können.

So konnten die zentralen Bestandteile einer Erklärung nach Art 86 AI Act durch dessen Zusammenschau mit den bestehenden datenschutzrechtlichen Regelungen in Verbindung mit Ableitungen aus Judikatur und Literatur sowie durch einen Blick auf den Entstehungsprozess dieser Norm herausgearbeitet werden. Dazu zählen einerseits zentrale Einflusskriterien, die für die Entscheidungsfindung herangezogen wurden, worunter insbesondere die Eingabedaten fallen. Zudem ist über die Gewichtung dieser Kriterien zu informieren sowie – soweit möglich – Auskunft darüber zu geben, welche Auswirkungen die Entscheidung auf die betroffene Person hat. Zwar muss die Erklärung keine Offenlegung des gesamten algorithmischen Codes, der dem System zugrunde liegt, beinhalten, jedoch Informationen über die algorithmische Gewichtung der wichtigsten Parameter, eine Beschreibung der Systemprozesse und eine Erklärung darüber, wie der eingesetzte Algorithmus grob operiert. Darüber hinaus konnten bereits formale Aspekte im Zusammenhang mit dem Recht auf Erklärung nach Art 86 AI Act behandelt und damit zusammenhängende weitere Informationspflichten abgehandelt werden.

Mögliche Abgrenzungsfragen wurden durch die ausgewählten Use Cases veranschaulicht und auf die praktische Ebene gehoben, um die teils abstrakten rechtlichen Ausführungen greifbarer zu machen. Die ausgewählten Fallbeispiele betrafen dabei die Preisbildung bei Lebens- und Krankenversicherung, Churn Predictions, Bonitäts- und Kreditwürdigkeitsprüfungen und die Emotionserkennung im Marketing bzw zur Absatzförderung mit insgesamt vier Unterfällen. Es konnte herausgearbeitet werden, dass sich die meisten der behandelten Use Cases Hochrisiko-KI-Systemen gem Art 6 Abs 2 iVm Anhang III AI Act zur Entscheidungsfindung bedienen und darüber hinaus die Voraussetzungen erfüllen, um in den Anwendungsbereich von Art 86 AI Act zu fallen. Es ist jedoch zu betonen, dass der gegenständliche Bericht angesichts der bisher spärlich bestehenden Literatur und mangelnden Judikatur zu Art 86 AI Act keine pauschale Einordnung von bestimmten Fallgruppen anstrebt und daher im Einzelfall zu prüfen sein wird, ob ein Fall vom Anwendungsbereich des AI Act und in weiterer Folge von Art 86 AI Act erfasst ist, wovon wiederum abhängt, ob einer betroffenen Person das Recht auf Erklärung zusteht. Zudem ist zu bedenken, dass Art 86 AI Act zum Zeitpunkt des Redaktionsschlusses des gegenständlichen Berichts (Februar 2025) noch nicht anwendbar war, und sich daher die noch erscheinende Literatur bzw künftige höchstgerichtliche

Rechtsprechung zu gewissen offenen Fragen noch äußern wird, weshalb sich der gegenständliche Bericht nicht als abschließende Analyse versteht und Perspektiven aus anderen Disziplinen miteinbezieht, um ein breiteres Bild des Rechts auf Erklärung zu zeichnen.

Einen über das Recht hinausgehenden Blick erlaubte dabei einerseits die Darstellung von relevanten sozialwissenschaftlichen Aspekten, wodurch zum einen zum Ausdruck kam, aus welchen Gründen dem bereits bestehenden Auskunftsrecht nach Art 15 DSGVO in der Praxis teilweise nicht nachgekommen wird, woraus wiederum Ableitungen für eine bessere praktische Durchsetzbarkeit von Art 86 AI Act getroffen werden können. Damit eng verknüpft wurde auf das Problem des sog „Automation Bias“ Bezug genommen, wonach häufig das Phänomen zu beobachten ist, dass sich Personen zu sehr auf automatisierte Entscheidungen verlassen, was die Notwendigkeit von Schulungen in diesem Bereich unterstreicht, insbesondere in Bezug auf KI-gestützte Entscheidungen, die den Auskunftsanspruch nach Art 86 AI Act auslösen. Ebenso zeigt dieses Phänomen auf, dass eine menschliche Überprüfung bei KI-gestützten Entscheidungen unbedingt erfolgen sollte (selbst wenn sie rechtlich nicht verbindlich oder in anderer Form vorgeschrieben ist), wobei auch darüber in der Erklärung nach Art 86 AI Act informiert werden sollte.

Abschließend wurden relevante ethische Aspekte des Rechts auf Erklärung vorgestellt, die sich zwar teilweise mit den rechtlichen Anforderungen decken, allerdings auch eine wertvolle Ergänzung zu diesen darstellen. So kann beispielsweise eine Erklärung des Betreibers über bestehende menschliche Verantwortungsketten ethisch sinnvoll sein, damit Betroffene das Zustandekommen der Entscheidung besser verstehen und dem KI-einsetzenden Unternehmen mehr Vertrauen entgegenbringen. Es ist daher zu empfehlen, diese der Erklärung nach Art 86 AI Act anzuschließen, selbst wenn dies nicht rechtlich vorgeschrieben ist. Weiters sollten Unternehmen Auskunft über die Rechtsgrundlagen geben, auf deren Basis die Entscheidungsfindung stattfindet, und die ethischen Überlegungen, die der Entscheidungsfindung zugrunde liegen, transparent machen. Darüber hinaus geben ethische Erwägungen Aufschluss über die generellen Schranken, die wir uns als Gesellschaft auferlegen wollen, welche insbesondere dann greifen, wenn ein Bereich angesichts des stetigen technologischen Fortschritts noch (rechtlich) unreguliert ist.

# 9 Anhang

## 9.1 Hochrisiko-KI-Systeme gem Anhang III AI Act

### 1. Biometrie

***Biometrie, soweit*** *ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht* ***zugelassen*** *ist:*

*a)* ***biometrische Fernidentifizierungssysteme****. Dazu gehören nicht KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, verwendet werden sollen;*

*b)* ***KI-Systeme****, die bestimmungsgemäß* ***für*** *die biometrische* ***Kategorisierung nach sensiblen*** *oder geschützten Attributen oder* ***Merkmalen*** *auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen;*

*c)* ***KI-Systeme****, die bestimmungsgemäß zur* ***Emotionserkennung*** *verwendet werden sollen.*

### 2. Kritische Infrastruktur

***KI-Systeme****, die bestimmungsgemäß als* ***Sicherheitsbauteile*** *im Rahmen der* ***Verwaltung*** *und des Betriebs* ***kritischer*** *digitaler* ***Infrastruktur****, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen.*

### 3. Allgemeine und berufliche Bildung

*a)* ***KI-Systeme****, die bestimmungsgemäß zur* ***Feststellung*** *des Zugangs oder der* ***Zulassung*** *oder zur Zuweisung natürlicher Personen zu Einrichtungen aller Ebenen der* ***allgemeinen*** *und* ***beruflichen Bildung*** *verwendet werden sollen;*

*b)* ***KI-Systeme****, die bestimmungsgemäß für die* ***Bewertung von Lernergebnissen*** *verwendet werden sollen, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern;*

*c)* ***KI-Systeme****, die bestimmungsgemäß zum Zweck der* ***Bewertung des angemessenen Bildungsniveaus****, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen;*

*d)* ***KI-Systeme****, die bestimmungsgemäß zur* ***Überwachung und Erkennung von verbotenem Verhalten*** *von Schülern* ***bei Prüfungen*** *im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen.*

**4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit**

*a)* ***KI-Systeme****, die bestimmungsgemäß für die* ***Einstellung oder Auswahl*** *natürlicher Personen verwendet werden sollen, insbesondere um gezielte* ***Stellenanzeigen*** *zu schalten,* ***Bewerbungen zu sichten*** *oder zu filtern und* ***Bewerber zu bewerten****;*

*b)* ***KI-Systeme****, die bestimmungsgemäß für* ***Entscheidungen****, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, für die* ***Zuweisung von Aufgaben*** *aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die* ***Beobachtung und Bewertung der Leistung*** *und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden sollen [Anmerkung: Fehler berichtigt].*

**5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen**

*a)* ***KI-Systeme,*** *die bestimmungsgemäß von* ***Behörden*** *oder im Namen von Behörden verwendet werden sollen, um zu* ***beurteilen****, ob natürliche Personen* ***Anspruch auf*** *grundlegende* ***öffentliche Unterstützungsleistungen*** *und -dienste, einschließlich* ***Gesundheitsdiensten****, haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind;*

*b)* ***KI-Systeme****, die bestimmungsgemäß für die* ***Kreditwürdigkeitsprüfung*** *und Bonitätsbewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden;*

*c)* ***KI-Systeme****, die bestimmungsgemäß für die* ***Risikobewertung und Preisbildung*** *in Bezug auf natürliche Personen im Fall von* ***Lebens- und Krankenversicherungen*** *verwendet werden sollen;*

*d)* ***KI-Systeme****, die bestimmungsgemäß zur* ***Bewertung und Klassifizierung von Notrufen*** *von natürlichen Personen oder für die Entsendung oder* ***Priorisierung*** *des Einsatzes von* ***Not- und Rettungsdiensten****, einschließlich Polizei, Feuerwehr und medizinischer Nothilfe, sowie für Systeme für die* ***Triage*** *von Patienten bei der Notfallversorgung verwendet werden sollen.*

## 6. Strafverfolgung

***Strafverfolgung, soweit*** *ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht* ***zugelassen*** *ist:*

***a)*** ***KI-Systeme****, die bestimmungsgemäß von* ***Strafverfolgungsbehörden*** *oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden oder in deren Namen zur* ***Bewertung des Risikos*** *einer natürlichen Person, zum* ***Opfer von Straftaten zu werden****, verwendet werden sollen;*

***b)*** ***KI-Systeme****, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden als Lügendetektoren oder ähnliche Instrumente verwendet werden sollen;*

***c)*** ***KI-Systeme****, die bestimmungsgemäß von* ***Strafverfolgungsbehörden*** *oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur* ***Bewertung der Verlässlichkeit von Beweismitteln*** *im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;*

***d)*** ***KI-Systeme****, die bestimmungsgemäß von* ***Strafverfolgungsbehörden*** *oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur* ***Bewertung des Risikos****, dass eine* ***natürliche Person eine Straftat begeht*** *oder erneut begeht, nicht nur auf der Grundlage der Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen verwendet werden sollen;*

***e)*** ***KI-Systeme****, die bestimmungsgemäß von* ***Strafverfolgungsbehörden*** *oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur* ***Erstellung von Profilen natürlicher Personen*** *gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der* ***Aufdeckung, Ermittlung oder Verfolgung*** *von* ***Straftaten*** *verwendet werden sollen.*

## 7. Migration, Asyl und Grenzkontrolle

***Migration, Asyl und Grenzkontrolle, soweit*** *ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht* ***zugelassen*** *ist:*

***a)*** ***KI-Systeme****, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder Organen, Einrichtungen und sonstigen Stellen der Union als* ***Lügendetektoren*** *verwendet werden sollen oder ähnliche Instrumente;*

*b)* ***KI-Systeme****, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur* ***Bewertung eines Risikos*** *verwendet werden sollen, einschließlich eines* ***Sicherheitsrisikos****, eines Risikos der* ***irregulären Einwanderung*** *oder eines* ***Gesundheitsrisikos****, das* ***von*** *einer natürlichen* ***Person ausgeht****, die in das Hoheitsgebiet eines Mitgliedstaats* ***einzureisen beabsichtigt*** *oder eingereist ist;*

*c)* ***KI-Systeme****, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union verwendet werden sollen, um zuständige Behörden bei der* ***Prüfung von Asyl- und Visumanträgen*** *sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen, einschließlich damit zusammenhängender* ***Bewertungen der Verlässlichkeit von Beweismitteln****, zu unterstützen;*

*d)* ***KI-Systeme****, die bestimmungsgemäß von oder im Namen der zuständigen Behörden oder Organen, Einrichtungen und sonstigen Stellen der Union, im Zusammenhang mit* ***Migration, Asyl oder Grenzkontrolle*** *zum Zwecke der* ***Aufdeckung, Anerkennung oder Identifizierung natürlicher Personen*** *verwendet werden sollen, mit Ausnahme der Überprüfung von Reisedokumenten.*

## 8. Rechtspflege und demokratische Prozesse

*a)* ***KI-Systeme****, die bestimmungsgemäß von einer oder im Namen einer* ***Justizbehörde*** *verwendet werden sollen, um eine Justizbehörde bei der Ermittlung und* ***Auslegung von Sachverhalten und Rechtsvorschriften*** *und bei der Anwendung des Rechts auf konkrete Sachverhalte zu unterstützen, oder die auf ähnliche Weise für die alternative Streitbeilegung genutzt werden sollen;*

*b)* ***KI-Systeme****, die bestimmungsgemäß verwendet werden sollen, um das* ***Ergebnis einer Wahl*** *oder eines* ***Referendums*** *oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum* ***zu beeinflussen****. Dazu gehören nicht KI-Systeme, deren Ausgaben natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung oder Strukturierung politischer Kampagnen in administrativer oder logistischer Hinsicht.*

## 9.2 Abkürzungsverzeichnis

| | |
|---|---|
| A29WP | Article 29 Data Protection Working Party (Artikel-29-Datenschutzgruppe) |
| ABl | Amtsblatt (der EU) |
| Abs | Absatz |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union |
| AI | Artificial Intelligence |
| AI Act | Artificial Intelligence Act (EU KI-Verordnung) |
| AI HLEG | Independent High-Level Expert Group on Artificial Intelligence („Unabhängige Expertengruppe für Künstliche Intelligenz“) |
| Anm | Anmerkung |
| Art | Artikel |
| BDSG | Bundesdatenschutzgesetz |
| bspw | beispielsweise |
| BVwG | Bundesverwaltungsgericht |
| et al | et alii, et aliae, et alia (und andere) |
| etc | et cetera |
| dh | das heißt |
| DSB | Datenschutzbehörde (Österreich) |
| DSG | Datenschutzgesetz (Österreich) |
| DSGVO | Datenschutz-Grundverordnung |
| DSRL-PJ | Datenschutzrichtlinie für den Bereich Polizei und Justiz |
| EDPB | European Data Protection Board (Englische Bezeichnung des EDSA) |
| EDSA | Europäischer Datenschutzausschuss |
| EES | Emotionserkennungssystem |
| EG-DSRL | EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) |

| | |
|---|---|
| EP | Europäisches Parlament |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| ErwGr | Erwägungsgrund |
| f | folgende |
| ff | fortfolgende |
| GA | Generalanwalt |
| GDPR | General Data Protection Regulation (Englische Bezeichnung der DSGVO) |
| gem | gemäß |
| GRC | Charta der Grundrechte der Europäischen Union |
| Hrsg | Herausgeber |
| iE | im Erscheinen |
| insb | insbesondere |
| iSd | im Sinne des |
| iSv | im Sinne von |
| iVm | in Verbindung mit |
| iZm | Im Zusammenhang mit |
| KI | Künstliche Intelligenz |
| lit | litera (Buchstabe) |
| mwN | mit weiteren Nachweisen |
| Rs | Rechtssache |
| RTE | Right to Explanation („Recht auf Erklärung“) |
| Rz | Randziffer |
| SA | Schlussanträge |
| sog | sogenannt |

| | |
|---|---|
| vgl | vergleiche |
| VO | (EU) Verordnung |
| VwG | Verwaltungsgericht |
| VwGH | Verwaltungsgerichtshof |
| XAI | eXplainable AI („Erklärbare KI“) |
| Z | Ziffer |
| zB | zum Beispiel |

**Research Institute – Digital Human Rights Center**

---

**Urheberrechtlicher Hinweis**:

Das Titelbild wurde KI generiert mittels Chat-GPT (DALL·E 3) sowie Adobe Express – es unterliegt daher keinem Urheberrecht.

https://researchinstitute.at

kontakt@researchinstitute.at

© 2025 RI – Alle Rechte vorbehalten