



Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutz bei
KI-Projekten in der
bayerischen Verwaltung
Orientierungshilfe

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagnmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
<https://www.datenschutz-bayern.de>

Bearbeitet von:

Dr. Verena Guttenberg, Deborah Kram, Angelika Lewinski,
Dr. Magdalena Schmidt, Dr. Christoph Wambsganz, Daniel Zapf

Version 1.0 | Stand: 1. März 2026

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt.
Es kann im Internet auf <https://www.datenschutz-bayern.de> in der Rubrik
„Infothek“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Die zunehmende Verbreitung und rasche Entwicklung Künstlicher Intelligenz (KI) wirkt sich immer stärker nicht nur auf die Gesellschaft und Arbeitswelt als Ganzes, sondern spezifisch auch auf die öffentliche Verwaltung aus. Dabei gehen die Entwicklung und die Nutzung von Künstlicher Intelligenz mit teils erheblichen tatsächlichen, ethischen und insbesondere rechtlichen Herausforderungen einher. Besondere Bedeutung kommt in diesem Zusammenhang dem Datenschutzrecht zu, welches immer dann zum Tragen kommt, wenn mittels Künstlicher Intelligenz personenbezogene Daten natürlicher Personen verarbeitet werden. Gleichzeitig trägt gerade das Datenschutzrecht mit seinen Anforderungen an Transparenz, Verständlichkeit und Nachvollziehbarkeit in besonderem Maße zu Vertrauensschutz und Menschenzentriertheit von Künstlicher Intelligenz bei.

Die vorliegende Orientierungshilfe möchte daher Künstliche Intelligenz für bayerische öffentliche Stellen aus der Perspektive des Datenschutzrechts erschließen und einordnen: Ausgehend vom Begriff der Künstlichen Intelligenz und dem unionalen Regelwerk der KI-Verordnung werden unter Einbeziehung von Chancen, Risiken, Problemen und Anwendungsfällen die einschlägigen datenschutzrechtlichen Anforderungen dargestellt und Vorschläge zum Umgang mit Künstlicher Intelligenz und deren Implementierung gemacht. Dabei stellt Künstliche Intelligenz, mittels derer personenbezogene Daten verarbeitet werden, aufgrund ihrer Vielfalt und Komplexität zwar ein durchaus anspruchsvolles datenschutzrechtliches Thema dar, unterliegt aber im Grundsatz den inzwischen über Jahre entwickelten und erprobten Mechanismen zur Umsetzung der Vorgaben insbesondere der Datenschutz-Grundverordnung.

Zugleich ist nicht nur der wissenschaftliche und technische Fortschritt Künstliche Intelligenz betreffend rasant, vielmehr unterliegen auch die regulatorischen Vorgaben für Künstliche Intelligenz einem steten Wandel: So wird beispielsweise die KI-Verordnung zum einen fortlaufend durch verschiedene Handreichungen der Kommission operationalisiert, zum anderen enthalten der Vorschlag für eine digitale Omnibus-Verordnung über KI¹ sowie der Vorschlag für eine Digital-Omnibus-Verordnung², jeweils vom 19. November 2025, Änderungsvorschläge der Kommission betreffend die KI-Verordnung sowie die Datenschutz-Grundverordnung. Vor diesem Hintergrund kann die Orientierungshilfe letztlich nur eine Momentaufnahme für den Zeitpunkt ihrer Veröffentlichung bieten. Der Leser bleibt zu einer

¹ Europäische Kommission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 19. November 2025, COM(2025) 836 final, Internet: <https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-ai-regulation-proposal>.

² Europäische Kommission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), 19.11.2025, COM(2025) 837 final, <https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-regulation-proposal>.

Vorwort

eigenständigen Reflektion des jeweils aktuellen Sach- und Rechtsstands aufgerufen. Für Rückfragen oder Verbesserungsvorschläge können Sie den Bayerischen Landesbeauftragten für den Datenschutz unter dem Postfach [**orientierungshilfen@datenschutz-bayern.de**](mailto:orientierungshilfen@datenschutz-bayern.de) erreichen.

Inhaltsverzeichnis

Vorwort.....	3
Inhaltsverzeichnis	5
I. Einführung.....	9
II. Begriffsbestimmung	11
III. KI-Verordnung.....	15
1. Verbotene KI-Praktiken (Art. 5 KI-Verordnung).....	18
2. Hochrisiko-KI-Systeme (Art. 6 KI-Verordnung)	21
3. KI-Systeme mit begrenztem Risiko (Art. 50 KI-Verordnung).....	27
4. KI-Systeme mit keinem oder geringem Risiko.....	28
5. Regulierung von KI-Modellen mit allgemeinem Verwendungszweck (Art. 51 ff. KI-Verordnung).....	29
6. KI-Kompetenz (Art. 4 KI-Verordnung)	31
7. Durchsetzung der KI-Verordnung	33
a) Büro für Künstliche Intelligenz (Art. 64 KI-Verordnung).....	33
b) Behörden in den Mitgliedstaaten.....	34
c) Rechtsdurchsetzung	36
8. Geplante Änderungen der KI-Verordnung	37
IV. Weitere Vorgaben des Unionsrechts und des nationalen Rechts.....	38
1. Unionsrecht.....	38
2. Nationales Recht.....	39
a) Dienstrecht	40
b) Verwaltungsrecht.....	41
V. Datenschutz-Grundverordnung.....	42
1. Verhältnis der Datenschutz-Grundverordnung zur KI-Verordnung.....	43
a) Allgemeines	43
b) Regelungen der KI-Verordnung im Bereich Datenschutz	43
c) Regelungen der Datenschutz-Grundverordnung im Bereich Künstliche Intelligenz	46
2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Systemen	48
a) Entwicklung von KI-Systemen.....	51
b) Training von KI-Systemen	51
aa) Erhebung von Trainings-, Test- und Validierungsdaten für KI-Systeme	53
bb) Aufbereitung von Daten für das Training von KI-Systemen	54
cc) Verarbeitung von Daten für das Training von KI-Systemen.....	54
dd) Fine-Tuning oder Nachtraining von KI-Systemen	55

Inhaltsverzeichnis

c)	Bereitstellung und Implementierung von KI-Systemen.....	55
d)	Nutzung von KI-Systemen.....	59
aa)	Eingabe (personenbezogener) Daten des Nutzers bei der Anmeldung bei einem KI-System.....	59
bb)	Eingabe (personenbezogener Daten) bei der Nutzung eines KI-Systems.....	60
cc)	Verarbeitung der eingegebenen Daten mit innerhalb eines KI-Systems vorhandenen Daten.....	60
dd)	Verarbeitung von spezifischen Betriebsmitteldaten beim Einsatz eines KI- Systems	62
ee)	Weiterverarbeitung der eingegebenen Daten zum Training eines KI-Systems	63
e)	Nutzung von Ergebnissen der Künstlichen Intelligenz	63
f)	Bereiche oder Phasen von KI-Systemen ohne personenbezogene Daten.....	64
3.	Datenschutzrechtliche Anforderungen im Einzelnen	64
a)	Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO)	64
aa)	Rechtmäßigkeit, Treu und Glauben, Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO).....	64
bb)	Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO)	65
cc)	Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO)	67
dd)	Richtigkeit (Art. 5 Abs. 1 Buchst. d DSGVO).....	67
ee)	Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO)	68
ff)	Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO).....	69
b)	Rechtsgrundlagen	69
aa)	Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO)	71
bb)	Aufgabenwahrnehmung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO).....	71
cc)	Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO)	73
dd)	Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO).....	76
ee)	Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO)	77
ff)	Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO).....	77
(1)	Einwilligung (Art. 9 Abs. 2 Buchst. a DSGVO).....	79
(2)	Veröffentlichung durch die betroffene Person (Art. 9 Abs. 2 Buchst. e DSGVO).....	80
(3)	Archiv-, Forschungs- oder statistische Zwecke (Art. 9 Abs. 2 Buchst. j DSGVO)	81
(4)	Art. 9 Abs. 2 Buchst. g DSGVO in Verbindung mit Art. 10 Abs. 5 KI-Verordnung.....	81
(5)	Zweckänderung (Art. 6 Abs. 4 DSGVO, Art. 6 Abs. 2 BayDSG).....	81
c)	Datenschutzrechtliche Verantwortlichkeit	82
aa)	Alleinige Verantwortlichkeit	83
bb)	Gemeinsame Verantwortlichkeit	85
cc)	Auftragsverarbeitung.....	87

Inhaltsverzeichnis

d) Weitere datenschutzrechtliche Aspekte.....	88
aa) Informationspflichten (Art. 12 ff. DSGVO)	88
bb) Betroffenenrechte.....	91
(1) Recht auf Auskunft (Art. 15 DSGVO).....	92
(2) Recht auf Berichtigung (Art. 16 DSGVO) und Recht auf Löschung (Art. 17 DSGVO).....	94
cc) Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO)	97
dd) Technische und organisatorische Datenschutzaspekte.....	103
ee) Datenschutz-Folgenabschätzung (Art. 35 DSGVO)	106
ff) Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)	108
gg) Drittlandübermittlungen (Art. 44 ff. DSGVO)	108
(1) Allgemein.....	108
(2) Sonderfall: Cloud.....	110
hh) Einbindung der/des behördlichen Datenschutzbeauftragten	111
VI. Umsetzungsempfehlungen.....	112
VII. Zusammenfassung.....	116

I. Einführung

Künstliche Intelligenz entwickelt sich rasant und birgt großes Potenzial als Schlüsseltechnologie für die Digitalisierung der Gesellschaft in vielen Lebensbereichen. **1**

So können die immer leistungsfähigeren Verfahren der Künstlichen Intelligenz beispielsweise nicht nur branchenübergreifend den Arbeitsalltag verändern, medizinische Diagnostik und Behandlungsprozesse verbessern sowie Kommunikation und Sicherheit fördern, sondern auch effizientes Verwaltungshandeln beschleunigen. Vor diesem Hintergrund zielt die Vorgabe in Art. 5 Abs. 1 Bayerisches Digitalgesetz (BayDiG) zur Digitalisierung von Prozessen in der bayerischen öffentlichen Verwaltung – wie Art. 5 Abs. 2 Satz 2 BayDiG zeigt – auch auf den Einsatz von Künstlicher Intelligenz, insbesondere im Rahmen von Clouddiensten (vgl. Art. 3 Abs. 1 BayDiG). Der Einsatz Künstlicher Intelligenz ist „durch geeignete Kontroll- und Rechtsschutzmaßnahmen“ abzusichern. **2**

Beispiele für die Unterstützung modernen und effizienten Verwaltungshandelns durch Künstliche Intelligenz sind etwa **3**

- die Erstellung von Zusammenfassungen langer Dokumente,
- die Aufbereitung von Rechercheergebnissen,
- die Erstellung von automatisierten Datenanalysen,
- die Erstellung von Formulierungsvorschlägen,
- die Erstellung von Grafiken, Bildern und Videos,
- das Erkennen von Handschriften, Objekten und symbolischen Darstellungen sowie
- Datenformatumwandlungen.

Im Kontakt der Verwaltung mit Bürgerinnen und Bürgern können sich möglicherweise unter anderem **4**

- Chatbots zur Erstbeantwortung von Bürgeranfragen und
- digitale Assistenten für die Bearbeitung von Anträgen

als Hilfestellung erweisen.³

Gleichzeitig stellt die Entwicklung Künstlicher Intelligenz die Gesellschaft vor neue Herausforderungen, vor allem in ethischer, in der Folge aber auch in rechtlicher Hinsicht. Künstliche Intelligenz muss stets vom Menschen her gedacht werden⁴ und vertrauenswürdig sein.⁵ **5**

³ Zum Ganzen Eichenhofer, Implikationen der „KI-Verordnung“ für Verwaltung und Verwaltungsgerichtsbarkeit, DVBl. 2024, S. 1519, 1522 ff.

⁴ Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade, Gemeinsame Erklärung des Europäischen Parlaments, des Rats und der Kommission vom 26. Januar 2022, COM(2022) 28 final, S. 2, Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022DC0028>.

⁵ Vgl. Rahmenübereinkommen des Europarates über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit, 5. September 2024, SEV Nr. 225, das als erster rechtsverbindlicher internationaler Vertrag sicherstellen soll, dass der Einsatz von KI-Systemen in vollem Umfang im Einklang mit

I. Einführung

Transparenz, Verständlichkeit und Nachvollziehbarkeit von Systemen der Künstlichen Intelligenz sind relevante Anforderungen, die sich insbesondere im Datenschutzrecht wiederfinden. Daher ist es besonders wichtig, datenschutzrechtliche Bestimmungen von der Planung über die Umsetzung bis zur Nutzung in jeder „Lebensphase“ eines KI-Systems zu berücksichtigen.⁶ Eine datenschutzfreundliche Gestaltung trägt – gerade im Rahmen der zunehmenden Digitalisierung – zum Vertrauen in Systeme und damit zu einer größeren Nutzerakzeptanz bei. Eine nachträgliche Implementierung von datenschutzrechtlichen Vorgaben in ein vorhandenes KI-System ist regelmäßig schwierig bis unmöglich. Sollen keine öffentlichen Mittel vergeudet werden, müssen die datenschutzrechtlichen Rahmenbedingungen also möglichst frühzeitig bedacht werden.

Menschenrechten, Demokratie und Rechtsstaatlichkeit steht. Dabei ist zu beachten, dass die Definition von „System der künstlichen Intelligenz“ in Art. 2 Rahmenübereinkommen nicht identisch mit der Begriffsbestimmung von „KI-System“ in Art. 3 Nr. 1 KI-Verordnung ist.

⁶ Vgl. hierzu allgemein Bayerischer Landesbeauftragter für den Datenschutz, Datenschutzkonzepte für Digitalisierungsvorhaben, Aktuelle Kurz-Information 64, Stand 09/2025, Internet: <https://www.datenschutz-bayern.de/infothek/>.

II. Begriffsbestimmung

Systeme und Modelle der Künstlichen Intelligenz sind omnipräsent. Allerdings fehlte es lange Zeit an einem einheitlichen Begriffsverständnis. Ein solches Verständnis ist aber für die Bewertung in rechtlicher und technischer Hinsicht wesentlich. **6**

Art. 3 Nr. 1 Verordnung über Künstliche Intelligenz⁷ (im Folgenden: KI-Verordnung) enthält nun erstmals eine gesetzliche Beschreibung des Phänomens „Künstliche Intelligenz“. Danach bezeichnet der Ausdruck „**KI-System**“ **7**

„ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann⁸ 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[.]“

Wesentliche Komponenten hiervon sind **KI-Modelle** (vgl. Erwägungsgrund [EG] 97 Sätze 5 bis 7 KI-Verordnung).⁹ Diese sollen im Folgenden – soweit nicht entsprechend spezifiziert – vom Begriff des „KI-Systems“ umfasst sein. **8**

Die weite Begriffsbestimmung des „KI-Systems“ ist zwar ausweislich Art. 3 KI-Verordnung auf „die Zwecke dieser Verordnung“ beschränkt, dürfte aber auch darüber hinaus prägend sein. **9**

EG 12 KI-Verordnung erläutert die Voraussetzungen des Art. 3 Nr. 1 KI-Verordnung näher und enthält in Satz 2 Halbsatz 2 eine Klarstellung dahingehend, dass sich der Begriff des „KI-Systems“ nicht auf Systeme bezieht, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen. Ein wesentliches Merkmal von KI-Systemen ist vielmehr die „Fähigkeit [...], Modelle oder Algorithmen oder beides aus Eingaben oder Daten abzuleiten“ (vgl. EG 12 Satz 4 KI-Verordnung). **10**

Vereinfacht ausgedrückt liegt Künstliche Intelligenz vor, wenn **Computersysteme Aufgaben ausführen können, die „normalerweise“ menschliche Intelligenz erfordern**. Das bedeu- **11**

⁷ Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABl. EU L 2024/1689 vom 12. Juli 2024, S. 1. Die Definition des KI-Systems zählte zu den umstrittensten Punkten im Gesetzgebungsverfahren. Letztlich konnte sich ein Vorschlag durchsetzen, der an die Definition der OECD angelehnt ist: OECD, Empfehlung des Rats zu künstlicher Intelligenz, 2019, S. 5, Internet: <https://www.oecd.org/berlin/presse/Empfehlung-des-Rats-zu-kuenstlicher-Intelligenz.pdf>.

⁸ Mit Blick auf die Regelungsziele der KI-Verordnung ist davon auszugehen, dass diese Voraussetzung die fakultative Lernfähigkeit von KI-Systemen und nicht deren zwingendes Vorliegen betrifft.

⁹ „Obwohl KI-Modelle wesentliche Komponenten von KI-Systemen sind, stellen sie für sich genommen keine KI-Systeme dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon“.

II. Begriffsbestimmung

tet, dass diese Systeme grundsätzlich – auch komplexere, nicht im Detail vorgegebene – Aufgaben selbstständig lösen, dass sie Situationen analysieren und Entscheidungen treffen, dass sie mit ihrer Umgebung interagieren, sich an diese anpassen können und bei alldem dazulernen – ähnlich wie Menschen. Anders als bei klassischen Automatisierungssystemen entsprechen die Entscheidungsergebnisse aber nur mit einer gewissen Wahrscheinlichkeit den Erwartungen, und der Entscheidungsweg lässt sich regelmäßig nicht exakt nachvollziehen. Gleichwohl weisen die zum jetzigen Zeitpunkt verfügbaren KI-Systeme bei der „Entscheidungssicherheit“ – auch im Vergleich mit der menschlichen Bearbeitung – bereits eine recht hohe empirische Qualität auf.

- 12 In einer **Entwurfssfassung**¹⁰ der **KI-Verordnung** fand sich in **Anhang I** noch eine Spezifizierung der Begriffsbestimmung dahin, dass folgende Techniken und Konzepte umfasst sein sollten:
- Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning),
 - Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme sowie
 - Statistische Ansätze, Bayessche Schätz- Such- und Optimierungsmethoden.
- 13 Diese Konkretisierungen sind in der in Kraft getretenen Fassung nicht mehr enthalten, erleichtern aber dennoch das Verständnis.
- 14 Am 4. Februar 2025 hat die Kommission nicht verbindliche Leitlinien zur Anwendung der Definition von KI-Systemen veröffentlicht.¹¹
- 15 Die derzeit wohl verbreitetsten KI-Systeme beruhen auf **maschinellern Lernen** in der Ausprägung des Deep Learning sowie auf **logik- und wissensbasierten Ansätzen** mit Expertensystemen als wichtigster Erscheinungsform. „Deep Learning“ beschreibt dabei ein künstliches „neuronales Netz“, bestehend aus Eingangsneuronen, Ausgangsneuronen und einem dazwischenliegenden „Hidden Layer“, zur Erfassung komplexer und hierarchischer Muster.
- 16 Grundsätzlich sind **verschiedene Ausprägungen** von Künstlicher Intelligenz möglich:
- **Nicht-generative Künstliche Intelligenz** dient beispielsweise zur Klassifizierung, Zusammenfassung oder Übersetzung von Inhalten.
 - Sogenannte **generative Künstliche Intelligenz** ist darauf trainiert, auf eine Anfrage ein Ergebnis zu liefern, das in Form und Inhalt den Ergebnissen ähnelt, die ein Mensch zu einer vergleichbaren Anfrage erarbeiten würde. Bei wiederholter gleicher Eingabe können

¹⁰ 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 vom 21. April 2021, COM(2021) 206 final. Abgeändert in der ersten Lesung des Europäischen Parlaments am 14. Juni 2023.

¹¹ C(2025) 5053 final, Internet: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>.

die Ergebnisse differieren. Beispiele für generative Künstliche Intelligenz sind Text-, Bild-, Ton-, Video- und Codegeneratoren wie unter anderem Large Language Models (LLM, deutsch: **Große Sprachmodelle**¹²). Diese können eine Datenquelle nutzen (unimodale Modelle) oder Informationen aus verschiedenen Datenquellen medienübergreifend kombinieren (multimodale Modelle). Sogenannte „Reasoning-Modelle“ sind sogar in der Lage, Denkprozesse durchzuführen.

- Zielt ein KI-System darauf ab, Problemlösungsstrategien zu entwickeln, nach denen es selbstständig tätig wird und dafür externe Werkzeuge benutzt,¹³ zum Beispiel indem es aus einer definierten Menge von Informationen diejenigen aufruft, die der Bearbeitung einer Anfrage am ehesten entsprechen, handelt es sich um einen sogenannten **künstlich intelligenten Agenten**.
- **Symbolische Intelligenz** schließlich bezeichnet diejenigen KI-Systeme, die anhand einer formalen Logik Ergebnisse in mehreren Schritten verknüpfen. Solche Verfahren werden eingesetzt, falls keine Daten für den Lernprozess vorhanden sind oder sich die Aufgabe in Form logischer Zusammenhänge darstellen lässt. Anwendungsfälle sind beispielsweise die automatische Fehlersuche in Fertigungsanlagen und Programme, die anhand von medizinischem Expertenwissen Diagnosen stellen.

Technisch können KI-Systeme unmittelbar auf dem Endgerät des Nutzers beziehungsweise Betreibers bereitgestellt werden, oder der Nutzer kann mit seinem Endgerät via Webplattform, Programmierschnittstelle oder innerhalb eines cloudbasierten Systems auf einen entsprechenden Dienst außerhalb seines Einwirkungsbereichs zugreifen. Bei dem genutzten Endgerät kann es sich dabei nicht nur um einen Computer handeln; durch die fortschreitende Miniaturisierung von Hardwarekomponenten und die Optimierung von Algorithmen ist es

17

¹² Eine gesetzliche Definition von „Großen Sprachmodellen“ existiert nicht, Anhang XIII Buchst. d KI-Verordnung nennt „die Ein- und Ausgabemodalitäten des Modells wie Text-Text (Große Sprachmodelle)“ allerdings als Kriterium für KI-Modelle mit allgemeinem Verwendungszweck. Allgemein wird unter „Großen Sprachmodellen“ die automatisierte Verarbeitung schriftlicher Texteingaben unter Zurückgreifen auf „Erlerntes“ mit einer Antwort als Ergebnis verstanden (Bitkom, Große Sprachmodelle, 2023, S. 4 ff., Internet: <https://www.bitkom.org/Bitkom/Publikationen/Grosse-Sprachmodelle-Ein-Ueberblick>). Das Adjektiv „groß“ grenzt auf der Grundlage der Anzahl von Parametern von „kleinen“ beziehungsweise „kompakten“ Sprachmodellen ab. Viele kleinere Sprachmodelle können zudem als spezialisierte Sprachmodelle bezeichnet werden, welche eigens für bestimmte Bereiche oder Aufgaben trainiert oder fein abgestimmt sind. Zu Großen Sprachmodellen umfassend Barberá, AI Privacy Risks & Mitigations – Large Language Models (LLMs), EDSA Support Pool of Experts Programme, Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0065>.

¹³ Regelmäßig durch eine Kommunikation von Großen Sprachmodellen mit anderen Komponenten wie Diensten (Funktionalitäten) oder Datenspeichern (Informationen), beispielsweise mittels Model Context Protocol (MCP), einem quelloffenen, technischen Quasi-Standard für eine Schnittstelle (basierend auf einem Client-Server-Modell). Die Nutzung agentischer KI-Systeme birgt spezifische Risiken hinsichtlich Prompt Injection (mit dem besonderen schädlichen Fall der Lethal Trifecta), bösartiger (MCP-)Server und Weitergabe personenbezogener Daten an die KI-Anbieter. Zum Ganzen Tremmel, Die Sicherheitsprobleme des Model Context Protocols, heise online 5. August 2025, Internet: <https://www.heise.de/ratgeber/Die-Sicherheitsprobleme-des-Model-Context-Protocols-10454915.html>.

II. Begriffsbestimmung

zwischenzeitlich auch möglich, KI-Funktionalitäten in eine Vielzahl von Geräten zu integrieren, darunter Smartphones, Wearables, Haushaltsgeräte und industrielle IoT¹⁴-Geräte.

- 18 Allen diesen Systemen ist gemeinsam, dass die sich aus der Begriffsbestimmung ergebende Ergebnisausgabe auf der Grundlage maschineller Informationsverarbeitung von erhaltenen Eingaben und eigenen Lernprozessen **in der Regel enorme Datenmengen voraussetzt**. Dieser Datenbestand in Form von Entwicklungs-, das heißt Trainings-, Test- und Validierungsdaten, sowie Eingabedaten enthält regelmäßig personenbezogene Daten und auch besondere Kategorien solcher Daten. Die Verarbeitung von (personenbezogenen oder nicht personenbezogenen) Daten im Lebenszyklus von KI-Systemen ist allerdings kein Bestandteil der Beschreibung eines KI-Systems nach der KI-Verordnung. Vielmehr wird die Verarbeitung personenbezogener Daten durch das Datenschutzrecht geregelt. Dies führt dazu, dass sich **der Anwendungsbereich der KI-Verordnung im Einzelfall mit dem des Datenschutzrechts** überschneidet.
- 19 Vor Darstellung der aus diesem Grund im Einzelfall zu beachtenden datenschutzrechtlichen Anforderungen (Abschnitt V) soll allerdings im Folgenden zunächst ein Überblick über das Regelwerk der neuen KI-Verordnung (Abschnitt III) und einiger weiterer unionaler Rechtsakte (Abschnitt IV) gegeben werden. Dieser Regelungsrahmen statuiert die rechtlichen und technisch-organisatorischen Voraussetzungen für den Einsatz von KI-Systemen als solchen und gilt auch für öffentliche Stellen, sofern diese als Betreiber KI-Systeme nutzen und ihren Beschäftigten die Nutzung ermöglichen oder sogar als Anbieter von KI-Systemen tätig werden.

¹⁴ IoT ist die Abkürzung für Internet of Things, das heißt Internet der Dinge, und beschreibt eine globale Infrastruktur, die physische und virtuelle Objekte vernetzt und zusammenarbeiten lässt.

III. KI-Verordnung

Die Europäische Union möchte im Bereich Datenwirtschaft und Künstliche Intelligenz den **Schutz der Grundrechte** der Unionsbürgerinnen und Unionsbürger mit der **Förderung von Innovation** durch Schaffung eines fairen und transparenten digitalen Binnenmarkts für Daten verbinden.¹⁵ So soll insbesondere die bessere (kommerzielle) Nutzbarmachung bislang ungenutzter Daten, von Informationen und des Potenzials der Künstlichen Intelligenz eine Vorangstellung der Europäischen Union in der globalen digitalen Landschaft etablieren.

Vor diesem Hintergrund zielt die KI-Verordnung darauf, den **Einsatz von Künstlicher Intelligenz sicherer und vertrauenswürdig** zu gestalten (vgl. Art. 1 Abs. 1, EG 8, EG 27 KI-Verordnung). Nachdem das Europäische Parlament am 13. März 2024 mehrheitlich für das Gesetz gestimmt hatte, folgte am 21. Mai 2024 auch die Billigung durch den Rat. Nach der Veröffentlichung im Amtsblatt der Europäischen Union am 12. Juli 2024 **ist die KI-Verordnung gemäß ihrem Art. 113 Abs. 1 am 1. August 2024 um 0:00 Uhr in Kraft getreten**.¹⁶ Ab diesem Zeitpunkt sind bis zum Geltungsbeginn **gestufte Umsetzungsfristen** vorgesehen, wobei im Grundsatz eine Übergangsfrist von 24 Monaten besteht, Art. 113 Abs. 3 KI-Verordnung.¹⁷

Hinweis: Parallel dazu wurde das **Rahmenübereinkommen des Europarates über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit** (SEV Nr. 225)¹⁸ verhandelt und am 5. September 2024 von der Europäischen Union, dem Vereinigten Königreich, den Vereinigten Staaten von Amerika und weiteren Staaten unterzeichnet.¹⁹ Es handelt sich um den ersten rechtsverbindlichen internationalen Vertrag, der einen Standard für vertrauenswürdige Künstliche Intelligenz setzen soll.

Räumlich-sachlich umfasst der Anwendungsbereich der KI-Verordnung nach **Art. 2 Abs. 1 KI-Verordnung** neben sämtlichen in der Union in Verkehr gebrachten oder in Betrieb genommenen KI-Systemen oder in Verkehr gebrachten KI-Modellen mit allgemeinem

¹⁵ So schon Europäische Kommission, Weißbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“, 19. Februar 2020, COM(2020) 65 final, Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0065>.

¹⁶ Zur Berechnung dieses Zeitpunkts siehe nur Gellermann, in: Streinz, EUV/AEUV, 3. Aufl. 2018, Art. 297 AEUV Rn. 8.

¹⁷ Einem von verschiedenen Interessenvertretern geforderten Moratorium hinsichtlich der Umsetzungsfristen der KI-Verordnung hatte die Europäische Kommission zunächst eine klare Absage erteilt, <https://www.reuters.com/world/europe/artificial-intelligence-rules-go-ahead-no-pause-eu-commission-says-2025-07-04/>. Vgl. aber nun den Vorschlag der Europäischen Kommission für flexiblere Umsetzungsfristen in Art. 1 Abs. 31 Digital Omnibus on AI (Fn. 1).

¹⁸ <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225>. Nach Billigung der Unterzeichnung im Namen der Europäischen Union durch das Europäische Parlament am 11. März 2026 (P10_TA[2026]0071, Internet: https://www.europarl.europa.eu/doceo/document/TA-10-2026-0071_DE.html) kann der Rat das Abkommen nun offiziell abschließen.

¹⁹ <https://www.coe.int/de/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature>.

III. KI-Verordnung

Verwendungszweck auch KI-Systeme, die nach dem Niederlassungsprinzip und dem Marktortprinzip der unionsrechtlichen Regulierung unterfallen.

- 24 Für sie legt die KI-Verordnung sektorübergreifend **harmonisierende Regeln und Anforderungen für den gesamten Lebenszyklus** fest – von der Entwicklung über das Inverkehrbringen und die Inbetriebnahme bis zum Betrieb selbst.²⁰ Die KI-Verordnung folgt dabei dem **Ansatz und der Systematik für Produktsicherheits- und Produkthaftungsgesetze**. Das heißt, sie reguliert nicht die Technologie als solche, sondern bestimmte Anwendungsfälle, adressiert spezifische Risiken²¹ durch Pflichten²² und nimmt entlang der KI-Wertschöpfungskette insoweit vordringlich die Anbieter von Künstlicher Intelligenz (Art. 3 Nr. 3 KI-Verordnung²³, „Provider“) in den Blick. Daneben gelten weitere Vorgaben auch für sogenannte Produkthersteller (vgl. Art. 2 Abs. 1 Buchst. e, Art. 3 Nr. 8 KI-Verordnung), Einführer (Art. 3 Nr. 6 KI-Verordnung), Händler (Art. 3 Nr. 7 KI-Verordnung) und Betreiber, das heißt Verwender (Art. 3 Nr. 4 KI-Verordnung²⁴, „Deployer“, beispielsweise eine öffentliche Stelle mit ihren nutzenden Beschäftigten); zusammengefasst die Akteure (Art. 3 Nr. 8 KI-Verordnung).

- 25 **Hinweise: Bayerische öffentliche Stellen**, die KI-Systeme im Rahmen ihrer Aufgabenerfüllung in eigener Verantwortung einsetzen, werden **vorrangig als Betreiber im Sinne von Art. 3 Nr. 4 KI-Verordnung** adressiert.

Es ist zudem grundsätzlich denkbar, dass bayerische öffentliche Stellen als Anbieter eines KI-Systems nach Art. 3 Nr. 3 KI-Verordnung tätig werden, insbesondere wenn sie selbst ein solches System entwickeln oder entwickeln lassen und es unter ihrem eigenen Namen zum Eigengebrauch in Betrieb nehmen; ein Inverkehrbringen ist nicht zwingend erforderlich.

Im Übrigen gilt, dass die KI-Verordnung **für Wirtschaft und öffentliche Hand** – mit Ausnahme der Besonderheit der Grundrechte-Folgenabschätzung in Art. 27 KI-Verordnung (hierzu näher Rn. 51) – **im Wesentlichen dieselben Anforderungen** statuiert.

²⁰ Umfassend Almada, Law & Compliance in AI Security & Data Protection, EDSA Support Pool of Experts Programme, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/law-compliance-ai-security-data_en.

²¹ Unter anderem Intransparenz, Diskriminierung, Unvorhersehbarkeit und Autonomie.

²² So etabliert die KI-Verordnung beispielsweise Vorgaben betreffend hinreichende Performanz, Robustheit, IT-Sicherheit sowie zur Herstellung von Transparenz entlang des KI-Lebenszyklus' sowie zwischen Anbietern und mitgliedstaatlichen Behörden.

²³ Danach ist „Anbieter“ „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“. Umfasst sind mithin nicht nur die Entwickler und Hersteller von Künstlicher Intelligenz, sondern auch diejenigen Personen oder Stellen, die eine Künstliche Intelligenz entwickeln lassen und diese dann auf den Markt bringen. Im Übrigen umfasst das Tatbestandsmerkmal der Inbetriebnahme ausweislich Art. 3 Nr. 11 KI-Verordnung auch die Bereitstellung zum Eigengebrauch.

²⁴ „Betreiber“ ist nach Art. 3 Nr. 4 KI-Verordnung „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“. Mit „Behörden“ in diesem Sinne sind dabei ausweislich EG 23 KI-Verordnung sowohl die Behörden der Mitgliedstaaten als auch der Union selbst gemeint.

Praxishinweis: Der Anwendungsbereich der Anbieterpflichten ist mit Blick auf die weite Begriffsbestimmung in Art. 3 Nr. 3, Nr. 11 KI-Verordnung sowie deren Zuweisung an andere Akteure nach Art. 25 KI-Verordnung unter Umständen schnell eröffnet. 26

Die Verordnung verfolgt dabei einen **risikobasierten Ansatz** und definiert zur Bewältigung der spezifischen Anforderungen, die KI-Systeme mit sich bringen können, **vier Risikostufen, für die jeweils unterschiedliche Vorgaben und Verpflichtungen gelten**, wobei die Anforderungen umso strenger sind, je risikoreicher das konkrete Einsatzfeld ist. Die **Einstufung hängt dabei insbesondere von der Zweckbestimmung und den konkreten Anwendungsbereichen** des jeweiligen KI-Systems ab und folgt dem ermittelten Risiko.²⁵ Unterschieden werden verbotene KI-Praktiken (Art. 5 KI-Verordnung), Hochrisiko-KI-Systeme (Art. 6 KI-Verordnung), KI-Systeme mit begrenztem Risiko (Art. 50 KI-Verordnung) und KI-Systeme mit keinem oder geringem Risiko (Art. 95 KI-Verordnung). Daneben stehen KI-Modelle mit allgemeinem Verwendungszweck (Art. 51 ff. KI-Verordnung). 27

In einem **ersten Schritt** ist daher zu prüfen, ob ein **KI-System im Sinne des Art. 3 Nr. 1 KI-Verordnung im Anwendungsbereich der KI-Verordnung** vorliegt, um in einem **zweiten Schritt** zu bestimmen, um **welche Art von KI-System es sich handelt und damit welche Anforderungen** eingehalten werden müssen.²⁶ 28

Ausgenommen vom Anwendungsbereich der KI-Verordnung sind nach **Art. 2 KI-Verordnung** unter anderem 29

- die Zuständigkeiten der Mitgliedstaaten im Hinblick auf die **nationale Sicherheit** (Art. 2 Abs. 3 UAbs. 1, EG 24 KI-Verordnung),²⁷
- KI-Systeme für ausschließlich **militärische oder verteidigungspolitische Zwecke** (Art. 2 Abs. 3 UAbs. 2, EG 24 KI-Verordnung),
- KI-Systeme oder KI-Modelle, die ausschließlich der **wissenschaftlichen Forschung und Entwicklung** dienen (Art. 2 Abs. 6, EG 25 KI-Verordnung),
- **Forschungs-, Test- und Entwicklungstätigkeiten** zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden, **ausgenommen Tests unter Realbedingungen** (Art. 2 Abs. 8, EG 25 KI-Verordnung),
- KI-Systeme, die **von natürlichen Personen im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit** verwendet werden (Art. 2 Abs. 10 KI-Verordnung), sowie

²⁵ Das heißt der Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens, Art. 3 Nr. 2 KI-Verordnung.

²⁶ Einen Ausgangspunkt für die Einrichtung eines Managementsystems für Künstliche Intelligenz kann dabei die internationale Norm ISO/IEC 42001:2023 darstellen, Internet: <https://www.iso.org/standard/81230.html>.

²⁷ Zur Eröffnung des Anwendungsbereichs der KI-Verordnung für die nationalen Polizei- und Sicherheitsbehörden sowie zum Harmonisierungsgrad der Vorschriften der KI-Verordnung in diesem Bereich Hofmann-Coombe, Die Anwendung der Unionsgrundrechte im Polizei- und Sicherheitsrecht nach der KI-VO, EuR 2025, S. 363, 365 ff.

III. KI-Verordnung

- KI-Systeme, die unter **freien und quelloffenen Lizenzen** bereitgestellt werden, **sofern diese nicht als Hochrisiko-KI-Systeme oder KI-Systeme nach Art. 5 oder Art. 50 KI-Verordnung** in Verkehr gebracht oder in Betrieb genommen werden (Art. 2 Abs. 12 KI-Verordnung).

1. Verbotene KI-Praktiken (Art. 5 KI-Verordnung)

30 Sogenannte unzulässige Künstliche Intelligenz sind die in Art. 5 Abs. 1 KI-Verordnung genannten verbotenen KI-Praktiken:

- **manipulative oder täuschende Techniken** zur unterschweligen Beeinflussung von Personen (Art. 5 Abs. 1 Buchst. a KI-Verordnung),
- **Ausnutzung der Schutzbedürftigkeit** einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation (Art. 5 Abs. 1 Buchst. b KI-Verordnung),
- **„Social Scoring“**²⁸ (Art. 5 Abs. 1 Buchst. c KI-Verordnung),
- **„Predictive Policing“**²⁹ (Art. 5 Abs. 1 Buchst. d KI-Verordnung),
- Erstellung oder Erweiterung von **Datenbanken zur Gesichtserkennung** (Art. 5 Abs. 1 Buchst. e KI-Verordnung),
- **Emotionserkennungssysteme** im Sinne des Art. 3 Nr. 39 KI-Verordnung am Arbeitsplatz und in Bildungseinrichtungen, sofern deren Verwendung nicht auf medizinischen Gründen oder Sicherheitsgründen beruht (Art. 5 Abs. 1 Buchst. f KI-Verordnung),
- **biometrische Kategorisierungen** im Sinne des Art. 3 Nr. 40 KI-Verordnung (Art. 5 Abs. 1 Buchst. g KI-Verordnung) sowie
- die Verwendung **biometrischer Echtzeit-Fernidentifizierungssysteme** in öffentlich zugänglichen Räumen im Sinne des Art. 3 Nr. 42 KI-Verordnung zu Zwecken der Strafverfolgung mit Ausnahme der unbedingten Erforderlichkeit für die Suche nach vermissten Personen, für die Verhinderung einer spezifischen und unmittelbar bevorstehenden terroristischen Bedrohung oder für das Aufspüren oder die Identifikation eines Verdächtigen einer schweren Straftat (Art. 5 Abs. 1 Buchst. h in Verbindung mit Anhang II KI-Verordnung).

31 **Hinweis:** Die Europäische Kommission hat am 4. Februar 2025 Leitlinien zur Anwendung der Verbote der KI-Verordnung veröffentlicht.³⁰ Deren formelle Annahme steht zwar noch aus.

²⁸ Bewertung von Personen anhand von persönlichen Merkmalen wie Geschlecht, Religion oder politische Überzeugung.

²⁹ Prognose der Wahrscheinlichkeit der Begehung einer Straftat einer Person ausschließlich auf der Grundlage der Erstellung eines Profils einer natürlichen Person oder der Bewertung ihrer Persönlichkeitsmerkmale und Eigenschaften.

³⁰ C(2025) 5052 final, Internet: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

1. Verbotene KI-Praktiken

Die Leitlinien stellen mit konkreten Beispielen und Erläuterungen zu verbotenen KI-Systemen aber bereits zum jetzigen Zeitpunkt eine wichtige Orientierungshilfe für die Praxis dar.

Bei auf solchen verbotenen Praktiken beruhenden KI-Systemen werden das **Inverkehrbringen, die Inbetriebnahme und die Verwendung, nicht allerdings die Entwicklung**, als **unvereinbar mit den Werten und Grundrechten der Europäischen Union** und daher als unzulässig angesehen. Der Nachweis der jedenfalls für Art. 5 Abs. 1 Buchst. a und b KI-Verordnung erforderlichen Beeinflussungsabsicht wird im Einzelfall allerdings nicht immer einfach sein. 32

Für das Verbot der Verwendung **biometrischer Echtzeit-Fernidentifizierungssysteme** im Sinne des Art. 3 Nr. 42 KI-Verordnung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken gelten gemäß **Art. 5 Abs. 2 bis 5 KI-Verordnung eng begrenzte Ausnahmen mit Mindestschutzmaßnahmen** (Art. 5 Abs. 2 KI-Verordnung),³¹ die unter dem Vorbehalt einer **vorherigen Genehmigung** durch eine nationale Justizbehörde oder unabhängige Verwaltungsbehörde stehen (Art. 5 Abs. 3 KI-Verordnung). Bei Regelung nationalrechtlicher Befugnisse zum Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme (die KI-Verordnung stellt insofern keine Rechtsgrundlage dar, vgl. EG 38 Satz 3 KI-Verordnung) müssen die Mitgliedstaaten diese Vorgaben beachten (vgl. Art. 5 Abs. 5 KI-Verordnung und die generellen Anforderungen des Art. 52 Charta der Grundrechte der Europäischen Union an grundrechtseinschränkende Regelungen). Zudem ist jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken nach **Art. 5 Abs. 4 Satz 1 KI-Verordnung** sowohl der zuständigen Marktüberwachungsbehörde auch als der nationalen **Datenschutzaufsichtsbehörde** mitzuteilen, welche wiederum der Kommission Jahresberichte über diese Verwendung vorzulegen haben (Art. 5 Abs. 6 Satz 1 KI-Verordnung). 33

Hinweis: Der Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zu einem anderen Zweck als dem der Strafverfolgung ist nicht als verbotene Praktik, sondern als Hochrisiko-KI eingestuft. Gleiches gilt für Fernidentifizierungssysteme, die – unabhängig vom Zweck – nicht in Echtzeit, sondern zur Identifikation ex post eingesetzt werden. Deren Verwendung muss allerdings nach Art. 26 Abs. 10 UAbs. 5 KI-Verordnung dokumentiert und auf Anfrage der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzaufsichtsbehörde zur Verfügung gestellt werden. Zudem müssen die Betreiber solcher Systeme den genannten Behörden gemäß Art. 26 Abs. 10 UAbs. 6 KI-Verordnung Jahresberichte vorlegen. 34

Ein Verstoß gegen das Verbot von unzulässigen KI-Praktiken im Sinne des Art. 5 KI-Verordnung ist **nach Art. 99 Abs. 3 KI-Verordnung bußgeldbewehrt**. Für die Einhaltung des Art. 5 KI-Verordnung gilt dabei nach **Art. 113 Abs. 3 Buchst. a KI-Verordnung** eine **Umsetzungsfrist von sechs Monaten ab Inkrafttreten** der Verordnung. 35

³¹ Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme im Hinblick auf die in Art. 5 Abs. 1 Buchst. h KI-Verordnung genannten Zwecke nur zur Bestätigung der Identität der speziell betroffenen Person unter Berücksichtigung der Art der Situation, die der möglichen Verwendung zugrunde liegt, sowie der Folgen der Verwendung des Systems für die Rechte und Freiheiten aller betroffenen Personen, unter Einhaltung notwendiger und verhältnismäßiger Schutzvorkehrungen und Bedingungen, insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen.

III. KI-Verordnung

- 36 Ein **Verbot** eines KI-Systems kann sich aber **auch aus anderen Vorschriften des Unionsrechts, namentlich dem Datenschutzrecht**,³² ergeben (vgl. **Art. 5 Abs. 8 KI-Verordnung**).

- 37 **Insbesondere Verhältnis zur Datenschutz-Grundverordnung: Art. 5 Abs. 1 Buchst. e KI-Verordnung** verbietet nur die Erstellung oder Erweiterung von Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen.³³ Das (un-)gezielte Auslesen anderer biometrischer Daten wie beispielsweise Stimmbilder („voice fingerprinting“) durch KI-Systeme verstößt allerdings regelmäßig gegen Datenschutzrecht, insbesondere gegen **Art. 9 und 10 Datenschutz-Grundverordnung (DSGVO)**, und ist aus diesem Grund rechtswidrig.³⁴

Art. 5 Abs. 1 Buchst. h KI-Verordnung untersagt beziehungsweise beschränkt bestimmte Verarbeitungen biometrischer Daten unabhängig von einem Personenbezug und dem verfolgten Ziel. Auf die Verarbeitung personenbezogener biometrischer Daten findet **Art. 9 DSGVO** dagegen zwar nur Anwendung, soweit diese Verarbeitung biometrischer (oder sonstiger besonderer Kategorien personenbezogener) Daten die eindeutige Identifizierung einer natürlichen Person bezweckt. In diesen Fällen ist die betreffende Verarbeitung durch die Datenschutz-Grundverordnung allerdings verboten. Dies gilt grundsätzlich auch für biometrische Fernidentifizierung.

Im Übrigen ist zu beachten, dass die **Definitionen des Begriffs „biometrische Daten“ in KI-Verordnung und Datenschutz-Grundverordnung sowie Datenschutz-Richtlinie für Polizei und Strafjustiz**³⁵ **nicht übereinstimmen**. Nach EG 14 KI-Verordnung soll der in der KI-Verordnung verwendete Begriff „biometrische Daten“ allerdings im Sinne der Begriffsbestimmung in Art. 4 Nr. 13 DSGVO, Art. 3 Nr. 18 Verordnung (EU) 2018/1725 sowie Art. 3 Nr. 13 JI-Richtlinie ausgelegt werden.

Generell ist die Nutzung der nach Art. 5 Abs. 1 KI-Verordnung verbotenen Systeme nicht nur mit den in der Charta der Grundrechte der Europäischen Union verankerten Werten unvereinbar, sondern im Einzelfall auch mit den Datenschutzgrundsätzen der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Erforderlichkeit sowie der Datenminimierung.

³² Europäische Kommission, Leitlinien zu verbotenen Praktiken der künstliche Intelligenz (KI) im Sinne des KI-Gesetzes, C(2025) 5052 final, Rn. 180, 221 (Fn. 30). Vgl. auch EG 28 KI-Verordnung.

³³ Vgl. auch Europäische Kommission, Leitlinien zu verbotenen Praktiken der künstliche Intelligenz (KI) im Sinne des KI-Gesetzes, C(2025) 5052 final, Rn. 234 (Fn. 30).

³⁴ Nach Auffassung des Europäischen Datenschutzbeauftragten könnten auch solche Verfahren vom Verbot des Art. 5 Abs. 1 Buchst. e KI-Verordnung erfasst sein, EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office, 19. Dezember 2024, S. 6, Internet: https://www.edps.europa.eu/data-protection/our-work/subjects/artificial-intelligence_en.

³⁵ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU L 119 vom 4. Mai 2016, S. 89.

2. Hochrisiko-KI-Systeme (Art. 6 KI-Verordnung)

Erfüllt ein KI-System die Voraussetzungen nach Art. 6 Abs. 1 in Verbindung mit Anhang I oder Art. 6 Abs. 2 in Verbindung mit Anhang III KI-Verordnung, gilt es als sogenanntes Hochrisiko-KI-System. Hochrisiko-KI-Systeme der zuletzt genannten Art stehen im **Zentrum der KI-Verordnung**; die Anforderungen an solche Systeme sind aufgrund deren möglicher Auswirkungen auf Grundrechte, Gesundheit oder Sicherheit umfassend. 38

Bei **Art. 6 Abs. 1 in Verbindung mit Anhang I KI-Verordnung** geht es um den Spezialfall der **Sicherheitskomponenten von Produkten, die unter die Harmonisierungsrechtsvorschriften der Union fallen, oder um diese Produkte selbst**, zum Beispiel Maschinen, Spielzeuge, Aufzüge, medizinische Geräte sowie Kraftfahrzeuge, land- und forstwirtschaftliche Fahrzeuge.³⁶ 39

Erhebliche Praxisauswirkungen wird dagegen **Art. 6 Abs. 2 in Verbindung mit Anhang III³⁷ KI-Verordnung** haben, wonach **eigenständige KI-Systeme in unter anderem den als schützenswert angesehenen Bereichen** Biometrie, Kritische Infrastrukturen, Bildung, Beschäftigung, Zugang zu grundlegenden privaten und öffentlichen Dienstleistungen, Strafverfolgung, Justiz, Migration und Grenzkontrolle als Hochrisiko-KI-Systeme einzuordnen sind, gegebenenfalls soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist.³⁸ Für den Fall, dass die betreffenden KI-Systeme **kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen** bergen, **indem sie unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflussen**,³⁹ statuiert **Art. 6 Abs. 3 UAbs. 1 KI-Verordnung** eine **Ausnahme** von dieser Regeleinordnung. 40

Hinweise: Für den Einsatz von KI-Systemen durch öffentliche Stellen ist stets sorgfältig zu prüfen, ob eine Einstufung als Hochrisiko-KI in Betracht kommt. Neben dem Einsatz von Künstlicher Intelligenz im Bereich der **Kritischen Infrastruktur** (Anhang III Nr. 2, EG 55 KI-Verordnung) ist dabei insbesondere an **Bildung** (Anhang III Nr. 3, EG 56 KI-Verordnung)⁴⁰, an **Beschäftigung und Personalmanagement** im Sinne des Anhangs III Nr. 4, EG 57 KI-Verordnung, an **Zugänglichkeit und Inanspruchnahme grundlegender** 41

³⁶ Als KI-Systeme fallen darunter beispielsweise virtuelle Assistenten oder Steuerungs- oder Überwachungssysteme als Teil solcher Produkte.

³⁷ Der EU-Kommission kommt insoweit gemäß Art. 7 KI-Verordnung eine Änderungsbefugnis unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien zu.

³⁸ Auch insoweit sind die Wertungen der Datenschutz-Grundverordnung zu beachten, insbesondere die Verarbeitungsgrundsätze der Rechtmäßigkeit sowie der Verarbeitung nach Treu und Glauben. So stehen insbesondere auf personenbezogene Daten gestützte „Vorhersagen“ im Rahmen der Strafverfolgung im Widerspruch zu den zentralen Grundsätzen der Unschuldsvermutung und der Nichtdiskriminierung. Dies hat wiederum Auswirkungen auf die Rechtmäßigkeit der Datenverarbeitung.

³⁹ Dabei ist unbeachtlich, ob es sich um menschliche oder automatisierte Entscheidungen handelt, vgl. EG 53 Satz 2 KI-Verordnung.

⁴⁰ Allgemein Lindner/Bode, Die Bedeutung der KI-VO der Europäischen Union für das Schulrecht, DÖV 2025, S. 462, sowie Kultusministerkonferenz, Handlungsempfehlung für die Bildungsverwaltung zum Umgang mit Künstlicher Intelligenz in schulischen Bildungsprozessen, Beschluss der Bildungsministerkonferenz vom 10. Oktober 2024, Internet: https://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2024/2024_10_10-Handlungsempfehlung-KI.pdf.

III. KI-Verordnung

öffentlicher Dienste und Leistungen nach Anhang III Nr. 5 Buchst. a und d, EG 58 KI-Verordnung (das heißt die Beurteilung von Ansprüchen auf grundlegende öffentliche Unterstützungsleistungen) sowie an **Strafverfolgung** (Anhang III Nr. 6, EG 59 KI-Verordnung), **Migration, Asyl und Grenzkontrolle** (Anhang III Nr. 7, EG 60 KI-Verordnung) sowie **Rechtspflege**⁴¹ und **demokratische Prozesse** (Anhang III Nr. 8, EG 61 KI-Verordnung) zu denken.

Anschließend ist im Einzelfall zu überlegen, ob der Einsatz von KI-Systemen in diesen Bereichen nur im Rahmen einer ergebnisoffenen Entscheidungsvorbereitung in internen Prozessen der Verwaltung erfolgt oder ob der Einsatz – wie regelmäßig anzunehmen sein wird – das Ergebnis der Entscheidungsfindung wesentlich beeinflusst und damit ein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt.

Eine ausweislich Art. 6 Abs. 5 KI-Verordnung eigentlich bis zum 2. Februar 2026 vorgesehene Veröffentlichung von Leitlinien der Kommission zur Einstufung von Hochrisiko-KI-Systemen und den damit verbundenen Anforderungen und Verpflichtungen steht derzeit noch aus.⁴²

- 42 **Art. 6 Abs. 3 UAbs. 2 KI-Verordnung** konkretisiert die Bedingungen für die Ausnahme des Art. 6 Abs. 3 UAbs. 1 KI-Verordnung auf **untergeordnete Hilfstätigkeiten** wie eng gefasste Verfahrensaufgaben (Art. 6 Abs. 3 UAbs. 2 Buchst. a, EG 53 Satz 4 KI-Verordnung), die Verbesserung des Ergebnisses einer zuvor abgeschlossenen menschlichen Tätigkeit (Art. 6 Abs. 3 UAbs. 2 Buchst. b, EG 53 Satz 8 KI-Verordnung), die Erkennung von Entscheidungsmustern oder Abweichungen von früheren Entscheidungsmustern, ohne eine menschliche Bewertung zu ersetzen oder zu beeinflussen (Art. 6 Abs. 3 UAbs. 2 Buchst. c, EG 53 Satz 11 KI-Verordnung), oder die Durchführung einer vorbereitenden Aufgabe für eine Bewertung (Art. 6 Abs. 3 UAbs. 2 Buchst. d, EG 53 Satz 13 KI-Verordnung). Nimmt ein in Anhang III KI-Verordnung aufgeführtes KI-System ein **Profiling** natürlicher Personen vor, gilt es dagegen **immer als hochriskant, Art. 6 Abs. 3 UAbs. 3 KI-Verordnung**.⁴³
- 43 Sollte ein Anbieter der Auffassung sein, ein in Anhang III KI-Verordnung aufgeführtes KI-System sei nicht hochriskant (regulierte Selbsteinschätzung), muss er diese Bewertung gemäß Art. 6 Abs. 4 Satz 1 KI-Verordnung dokumentieren und das KI-System nach Art. 49 Abs. 2 KI-Verordnung registrieren (Art. 6 Abs. 4 Satz 2 KI-Verordnung).
- 44 Die Klassifizierung als Hochrisiko-KI-System ist mit **erheblichen Anforderungen an das KI-System** verbunden (**Art. 8 bis 15 KI-Verordnung**), die sowohl vor Inverkehrbringen als auch während des gesamten Lebenszyklus' des KI-Systems erfüllt sein müssen: So werden neben der Pflicht zur **Einrichtung eines Risikomanagementsystems** gemäß Art. 9 KI-Verordnung

⁴¹ Vgl. hierzu UNESCO, Guidelines für the use of AI systems in courts and tribunals, Internet: <https://unesdoc.unesco.org/ark:/48223/pf0000396582>; Europäische Kommission für die Wirksamkeit der Justiz, Guidelines on the use of generative artificial intelligence for courts, CEPEJ(2025)18Final, 19. Dezember 2025, Internet: <https://rm.coe.int/cepej-2025-18final-en-draft-guidelines-on-the-use-of-generative-ai-for/48802a4ad1>; Wachter/Leeb, KI-Systeme in der Rechtspflege, RD 2024, S. 440.

⁴² Zum Konsultationsverfahren <https://digital-strategy.ec.europa.eu/de/news/commission-launches-public-consultation-high-risk-ai-systems>.

⁴³ Zum Verhältnis von Art. 6 Abs. 3 UAbs. 3 KI-Verordnung und Art. 22 DSGVO Steenbergen, Datenschutzrechtliche Entscheidungsfindungen als Hochrisiko-KI-Systeme, KIR 2025, 326.

als zentralem Element⁴⁴ **Anforderungen an die Daten und Daten-Governance** (Art. 10 KI-Verordnung), an die Erstellung und Aufbewahrung **technischer Dokumentation** (Art. 11 und 12 KI-Verordnung), an die **Informationsbereitstellung** (Art. 13 KI-Verordnung, „Betriebsanleitungen“)⁴⁵, an die **Sicherstellung menschlicher Aufsicht** („human in the loop“, Art. 14, Art. 26 Abs. 2 KI-Verordnung) sowie an die **Genauigkeit, Robustheit und Cybersicherheit** des KI-Systems (Art. 15 KI-Verordnung) etabliert.⁴⁶

Hinweise: Die genannten Anforderungen können bei Verarbeitung personenbezogener Daten im Zusammenhang mit dem KI-System von den datenschutzrechtlich Verantwortlichen unterstützend zur Erfüllung der Transparenz- und Rechtmäßigkeitsanforderungen der Datenschutz-Grundverordnung herangezogen werden.⁴⁷

45

In diesem Zusammenhang ist zu beachten, dass die Vorgabe des **Art. 14 (sowie des Art. 26 Abs. 2) KI-Verordnung** zur Sicherstellung menschlicher Aufsicht für sämtliche Hochrisiko-KI-Systeme gilt und damit einen **weiteren Anwendungsbereich** hat als die entsprechende **Vorgabe im Zusammenhang mit automatisierten Entscheidungen nach Art. 22 Abs. 1 DSGVO**. Letztere wiederum findet unabhängig davon Anwendung, ob es sich bei dem personenbezogene Daten verarbeitenden System um ein System der Künstlichen Intelligenz handelt oder nicht. Die Erfüllung der Anforderungen der Art. 14, Art. 26 Abs. 2 KI-Verordnung kann allerdings eine „Vor-Voraussetzung“ für die Verpflichtungen nach Art. 22 DSGVO sein.

Ebenso erfüllen die ordnungsgemäße Einhaltung der Vorgaben des Art. 22 DSGVO und der zugehörigen Informationspflichten aus Art. 13 Abs. 2 Buchst. f, Art. 14 Abs. 2 Buchst. g, Art. 15 Abs. 1 Buchst. h DSGVO das die Verpflichtung zur Sicherstellung menschlicher Aufsicht flankierende **Recht der betroffenen Personen auf (ex post)⁴⁸ Erläuterung der Entscheidungsfindung im Einzelfall⁴⁹ nach dem insoweit subsidiären Art. 86 KI-Verordnung** (vgl. Art. 86 Abs. 3 KI-Verordnung).⁵⁰

Anbieter, Betreiber (siehe Art. 25 und Art. 26 KI-Verordnung in Verbindung mit Art. 3 Nr. 23 KI-Verordnung), Einführer (siehe Art. 23 KI-Verordnung) und Händler (siehe Art. 24 KI-

46

⁴⁴ Die Risikoanalyse soll dabei die Gefahren im Hinblick auf Gesundheit, Sicherheit oder Grundrechte berücksichtigen, die das betreffende KI-System bei einer mit dem vorgesehenen Zweck übereinstimmenden Verwendung mit sich bringt.

⁴⁵ Spezifikationen hierzu finden sich in ISO/IEC TS 6254:2025 (Information technology – Artificial intelligence – Objectives and approaches for explainability and interpretability of machine learning [ML] models and artificial intelligence [AI] systems), Internet: <https://www.iso.org/standard/82148.html#lifecycle>.

⁴⁶ Zur Umsetzung Buscemi/Deckenbrunnen/Kabir/Mishchenko/Mowla, Assessing High-Risk AI Systems under the EU AI Act: From Legal Requirements to Technical Verifications, arXiv:2512.13907, Internet: <https://arxiv.org/abs/2512.13907>.

⁴⁷ Hierzu auch Hansen, Dokumentation als Normalfall?, DuD 2025, S. 288.

⁴⁸ Vgl. Kasper, Die Verwaltung in der KI-Regulierung – Gesichtspunkte bei Betreiben, Nutzen und Beaufsichtigen von KI-Systemen –, DÖV 2025, S. 471, 480 m. w. N.

⁴⁹ Mit Blick auf den Regelungszweck des Art. 86 KI-Verordnung kann zur Auslegung der Tatbestandsmerkmale auf die Rechtsprechung des EuGH zum Auskunftsrecht nach Art. 15 Abs. 1 Buchst. h in Verbindung mit Art. 22 DSGVO zurückgegriffen werden (EuGH, Urteil vom 27. Februar 2025, C-203/22, hierzu näher unten Rn. 338). Konkret zur Auslegung von Art. 86 KI-Verordnung bei automatisierten Entscheidungen hat der EuGH im Verfahren C-806/24 auf ein Vorabentscheidungsersuchen aus Bulgarien hin zu entscheiden.

⁵⁰ Zu Art. 86 KI-Verordnung ausführlich Hornung, Individualrechte in der KI-Verordnung, DuD 2024, S. 507.

III. KI-Verordnung

Verordnung) von Hochrisiko-KI treffen zudem zahlreiche **Pflichten (Art. 16 bis Art. 28, Art. 72⁵¹ und Art. 73⁵² KI-Verordnung)**.

- 47 **Hinweise zu Informationspflichten: Öffentliche Stellen als Beschäftigungsgeber** müssen insbesondere die für alle Arbeitgeber **geltende Informationspflicht nach Art. 26 Abs. 7 KI-Verordnung** beachten: Danach müssen Betreiber, die Beschäftigungsgeber sind, vor der Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz die Beschäftigtenvertreter und die betroffenen Beschäftigten über den geplanten Einsatz informieren.

Allgemeiner ist – unbeschadet Art. 50 KI-Verordnung – die nach Art. 26 Abs. 11 KI-Verordnung geltende Informationspflicht der Betreiber der in Anhang III KI-Verordnung aufgeführten Hochrisiko-KI-Systeme gegenüber den natürlichen Personen, die Gegenstand von Entscheidungen beziehungsweise Entscheidungsunterstützung durch das Hochrisiko-KI-System sind. Datenschutzrechtlich sind in diesem Kontext die Informationspflichten nach Art. 13 Abs. 2 Buchst. f und Art. 14 Abs. 2 Buchst. g DSGVO zu beachten.

- 48 Zum Nachweis, dass die Anforderungen erfüllt werden, muss der Anbieter der betreffenden Hochrisiko-KI (gegebenenfalls erneut, Art. 43 Abs. 4 KI-Verordnung) eine interne **Konformitätsbewertung** (Art. 43 Abs. 1 UAbs. 1 Buchst. a, Abs. 2 in Verbindung mit Anhang VI KI-Verordnung) für sein KI-System vornehmen, wobei eine solche – insbesondere unter bestimmten Voraussetzungen bei Hochrisiko-KI im Bereich Biometrie (vgl. Art. 43 Abs. 2 KI-Verordnung) – bei einer Konformitätsbewertungsstelle⁵³ einzuholen (Art. 43 Abs. 1 UAbs. 1 Buchst. b, Art. 30, EG 123 in Verbindung mit Anhang VIII KI-Verordnung) oder in Bezug auf von Anhang I erfasste Systeme zusätzlich das einschlägige Konformitätsbewertungsverfahren durchzuführen ist (Art. 43 Abs. 3 KI-Verordnung). Zudem muss der Anbieter eine **EU-Konformitätserklärung** ausstellen (Art. 47 KI-Verordnung), eine (physische oder digitale) **CE-Kennzeichnung** an das Hochrisiko-KI-System anbringen (Art. 48 KI-Verordnung) und das KI-System **in einer EU-Datenbank** (mit einem sicheren nicht öffentlichen Teil für Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle)

⁵¹ Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme.

⁵² Meldung schwerwiegender Vorfälle. Hierzu hat die Kommission am 26. September 2025 den Entwurf von Leitlinien sowie einer Meldevorlage veröffentlicht, zu denen im Rahmen einer öffentlichen Konsultation bis zum 7. November 2025 Feedback gegeben werden kann, Internet: <https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks>.

⁵³ Die Konformitätsbewertungsstellen werden auf Antrag (Art. 29 KI-Verordnung) nach Art. 28 Abs. 1 KI-Verordnung von den sogenannten notifizierenden Behörden benannt und notifiziert. Wer diese Aufgabe in Deutschland wahrnehmen wird, ist noch nicht abschließend geklärt; zu notifizierenden Behörden vgl. aber Gesetzentwurf der Bundesregierung § 3 Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Gesetz zur Durchführung der Verordnung über künstliche Intelligenz), Bearbeitungsstand: 10. Februar 2026, Internet: https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/260209_RegE_KI-MIG_final_barr.pdf.

2. Hochrisiko-KI-Systeme

registrieren (Art. 49 KI-Verordnung). Art. 46 KI-Verordnung legt eng begrenzte Ausnahmen vom Konformitätsbewertungsverfahren fest.

Hinweise: Die **EU-Konformitätserklärung** muss nach **Art. 47 Abs. 2 KI-Verordnung** feststellen, dass das betreffende Hochrisiko-KI-System die in Abschnitt 2 KI-Verordnung festgelegten Anforderungen erfüllt. Dies **umfasst ausweislich Anhang V Nr. 5 KI-Verordnung auch die Datenschutzkonformität des Systems**. Dies betrifft nicht nur die datenschutzkonforme Entwicklung des Systems, sondern auch dessen datenschutzkonformen Einsatz, das heißt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Zusammenhang mit dem Hochrisiko-KI-System.

49

Zu den bei der Registrierung zu machenden Angaben gehört nach **Art. 49 in Verbindung mit Art. 71, Anhang VIII Abschnitt C Nr. 5 KI-Verordnung** gegebenenfalls eine **Zusammenfassung der im Einklang mit Art. 35 DSGVO gemäß Art. 26 Abs. 9 KI-Verordnung durchgeführten Datenschutz-Folgenabschätzung**.

Praxishinweis: Öffentliche Stellen sollten bei der Beschaffung von Hochrisiko-KI-Systemen im Wege der öffentlichen Vergabe darauf achten, sämtliche beschriebenen Pflichten in der Leistungsbeschreibung abzubilden.⁵⁴ In Bezug auf die Vorgaben der KI-Verordnung sollen öffentliche Auftraggeber dabei durch die von der Kommission zur Verfügung gestellten „Standardvertragsklauseln für die Beschaffung von KI-Systemen“ unterstützt werden.⁵⁵

50

Bestimmte **Auswirkungen auf die Grundrechte natürlicher Personen** können erst bei Inbetriebnahme eines KI-Systems eingeschätzt werden; deswegen müssen manche Betreiber⁵⁶ von Hochrisiko-KI-Systemen vor deren Inbetriebnahme gemäß **Art. 27 KI-Verordnung** eine – durch die KI-Verordnung **neu** eingeführte – **Grundrechte-Folgenabschätzung** vornehmen, das heißt eine Abschätzung der Auswirkungen, die die Verwendung des betreffenden KI-Systems auf die – in der Charta der Grundrechte der Europäischen Union verankerten – Grundrechte natürlicher Personen haben kann.⁵⁷ Verpflichtet hierzu sind nach Art. 27 Abs. 1 Satz 1 KI-Verordnung **Einrichtungen des öffentlichen Rechts**, private Einrichtungen, die öffentliche Dienste erbringen, sowie private Betreiber in den Hochrisiko-Anwendungsfällen „Kreditwürdigkeitsprüfung“ sowie „Kranken- und Lebensversicherung“. Ob der geplante KI-Einsatz zur Erfüllung öffentlicher Aufgaben vorgenommen wird, ist dagegen nicht entscheidend. Gemäß Art. 27 Abs. 1 Satz 2 KI-Verordnung muss die Grundrechte-Folgenabschätzung insbesondere eine Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird, die Kategorien von betroffenen Personen und Personengruppen, die spezifischen Schadensrisiken, die Umsetzung von Maßnahmen der menschlichen Aufsicht sowie die Maßnahmen, die bei Eintreten der Schadensrisiken zu ergreifen sind, umfassen; hierbei können nach EG 96

51

⁵⁴ Hierzu Horn/Schuchert, Staatliche Beschaffung von KI-Systemen, MMR 2024, S. 926.

⁵⁵ Internet: <https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai>.

⁵⁶ Dies muss mit Blick auf die Grundrechtsgebundenheit öffentlicher Stellen und unter Berücksichtigung von EG 83 Satz 3 KI-Verordnung auch für Betreiber gelten, die das betreffende Hochrisiko-KI-System selbst entwickelt haben beziehungsweise haben entwickeln lassen.

⁵⁷ Unterstützend kann hier möglicherweise die im Mai 2025 veröffentlichte ISO/IEC 42005:2025 zur Durchführung von Auswirkungenanalysen von KI-Systemen herangezogen werden, Internet: <https://www.iso.org/standard/42005>.

III. KI-Verordnung

Satz 11 KI-Verordnung auch relevante Interessenträger, unabhängige Sachverständige und Organisationen der Zivilgesellschaft einbezogen werden. Art. 27 KI-Verordnung geht insoweit **über die allgemeinen Vorgaben zur Risikobewertung in Art. 9 KI-Verordnung hinaus**. Der Betreiber des Hochrisiko-KI-Systems muss der zuständigen Marktüberwachungsbehörde das Ergebnis der Grundrechte-Folgenabschätzung mitteilen, Art. 27 Abs. 1 KI-Verordnung, mit Ausnahme für den in Art. 46 Abs. 1 KI-Verordnung genannten Fall. Bei Änderung oder Aktualisierung eines der in Art. 27 Abs. 1 KI-Verordnung aufgeführten Elemente muss auch die Grundrechte-Folgenabschätzung aktualisiert werden, Art. 27 Abs. 2 Satz 3 KI-Verordnung.

- 52 **Hinweis:** Zeitlich vor dieser Grundrechte-Folgenabschätzung muss **bei Verarbeitung personenbezogener Daten gegebenenfalls nach Art. 35 DSGVO eine Datenschutz-Folgenabschätzung** durchgeführt werden – zumindest vor Entwicklung eines Hochrisiko-KI-Systems und gegebenenfalls noch einmal vor dessen Implementierung und Inbetriebnahme. Im Einzelfall ist es empfehlenswert, die beiden Folgenabschätzungen zu **koordinieren**; insbesondere kann die Grundrechte-Folgenabschätzung nach dem Willen des Unionsgesetzgebers nach **Art. 27 Abs. 4 KI-Verordnung** eine Datenschutz-Folgenabschätzung ergänzen.

Ein System, das als Hochrisiko-KI einzustufen ist, bringt zwar nicht zwingend ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen durch die Verarbeitung personenbezogener Daten mit sich und umgekehrt. Die Einstufung hat aber eine gewisse Indizwirkung.

- 53 **Art. 6 Abs. 1 KI-Verordnung** und die entsprechenden Pflichten müssen nach Art. 113 Abs. 3 Buchst. c KI-Verordnung innerhalb von **36 Monaten** nach Inkrafttreten der Verordnung erfüllt werden, **im Übrigen** findet die **allgemeine Umsetzungsfrist** des Art. 113 Abs. 1 KI-Verordnung Anwendung. Für **vor dem 2. August 2026 bereits auf dem Markt** befindliche Hochrisiko-KI-Systeme gilt nach Art. 111 Abs. 2 Satz 1 KI-Verordnung ein **gewisser Bestandsschutz, mit Einschränkungen für bestimmungsgemäß von Behörden verwendete Systeme** in Art. 111 Abs. 2 Satz 2 KI-Verordnung. Verstöße gegen Anforderungen an Hochrisiko-KI-Systeme sind nach **Art. 99 Abs. 4 Buchst. a bis e KI-Verordnung** **bußgeldbewehrt**.

- 54 **Hinweise:** Auch wenn die Vorgaben der KI-Verordnung zu Hochrisiko-KI gestuft über einen längeren Zeitraum bis 2. August 2026⁵⁸ in Kraft treten, empfiehlt es sich für öffentliche Stellen, bei entsprechender Einordnung der geplant einzusetzenden KI-Systeme die **jeweiligen Vorgaben vorgehend** schon vor dem jeweiligen Geltungsbeginn nach Art. 113 KI-Verordnung in der Planungs- und Entwicklungsphase umzusetzen und beispielsweise die Grundrechte-Folgenabschätzung nach Art. 27 KI-Verordnung durchzuführen.

Das Büro für Künstliche Intelligenz (hierzu Rn. 84 f.) ist nach **Art. 27 Abs. 5 KI-Verordnung** verpflichtet, ein **Muster für einen Fragebogen – auch mithilfe eines automati-**

⁵⁸ Vgl. aber nun den Vorschlag der Europäischen Kommission für flexiblere Umsetzungsfristen in Art. 1 Abs. 31 Digital Omnibus on AI (Fn. 1): Geltungsbeginn von Kapitel III Abschnitte 1, 2 und 3 ab dem 2. Dezember 2027 in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 2 und Anhang III als hochriskant eingestuft sind, und 2. August 2028 in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 1 und Anhang I als hochriskant eingestuft sind.

sierten Instruments – auszuarbeiten, um die Betreiber in die Lage zu versetzen, ihren Pflichten aus Art. 27 KI-Verordnung in vereinfachter Weise nachzukommen.

3. KI-Systeme mit begrenztem Risiko (Art. 50 KI-Verordnung)

Ein „begrenztes Risiko“ im Sinne der KI-Verordnung bezieht sich auf die **Risiken, die – unabhängig von der Verarbeitung personenbezogener Daten – mit mangelnder Transparenz bei der KI-Nutzung verbunden sind, wie Nachahmung, Manipulation oder Täuschung**, beispielsweise im Zusammenhang mit Chatbots, Deepfakes („tiefe Fälschungen“) oder KI-generierten Inhalten (vgl. EG 132 KI-Verordnung). 55

Die KI-Verordnung führt daher in **Art. 50 Abs. 1** zu einem **spezifische Transparenzpflichten für Anbieter und Betreiber von KI-Systemen ein, welche für die direkte Interaktion mit natürlichen Personen bestimmt sind**, um sicherzustellen, dass Menschen bei Bedarf informiert werden und Vertrauen gefördert wird: Diese KI-Systeme müssen so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich, Art. 50 Abs. 1 Satz 1 Halbsatz 2, EG 132 Satz 3 KI-Verordnung. Wann dies der Fall ist, erläutert die KI-Verordnung nicht näher. Wenn die Transparenzpflichten nicht unterlaufen werden sollen, ist diese Person eher mit einem durchschnittlich (un)erfahrenen IT-Nutzer als mit einem „KI-Nerd“ gleichzusetzen. 56

Beispiel: So müssen Menschen bei der Verwendung von KI-Systemen wie Chatbots grundsätzlich darauf aufmerksam gemacht werden, dass sie mit einer Maschine interagieren, damit sie eine informierte Entscheidung treffen können, fortzufahren oder den Prozess abzubrechen.

Dies gilt **unbeschadet der Transparenzanforderungen** für den Betreiber (als für die Verarbeitung Verantwortlichen), **die sich aus der Datenschutz-Grundverordnung ergeben (Art. 50 Abs. 6, EG 137 KI-Verordnung)**. 57

Nach den folgenden Absätzen des Art. 50 KI-Verordnung müssen Anbieter zum anderen sicherstellen, dass **KI-generierte Inhalte in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert identifizierbar** sind (**Art. 50 Abs. 2, EG 133⁵⁹ KI-Verordnung mit Ausnahmen in Art. 50 Abs. 2 Satz 3 KI-Verordnung**). Außerdem muss **KI-generierter Text**, der mit dem Ziel veröffentlicht wird, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, vom Betreiber **als künstlich erzeugt gekennzeichnet** werden (**Art. 50 Abs. 4 UAbs. 2 Satz 1 KI-Verordnung mit Ausnahmen in Art. 50 Abs. 4 UAbs. 2 Satz 2, EG 134 Satz 4 KI-Verordnung**). Dies gilt auch für Audio- und Videoinhalte, die **Deepfakes** im Sinne des **Art. 3 Nr. 60 KI-Verordnung** darstellen (**Art. 50 Abs. 4 UAbs. 1 KI-Verordnung**). Auf diese Weise soll Missbrauch und 58

⁵⁹ EG 133 Satz 4 KI-Verordnung nennt als mögliche Techniken in diesem Zusammenhang „Wasserzeichen, Metadatenidentifizierungen, kryptographische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden, Fingerabdrücke oder andere Techniken oder eine Kombination solcher Techniken je nach Sachlage“.

III. KI-Verordnung

Manipulation sowie Verletzungen des Persönlichkeitsrechts, etwa durch Fake News, das heißt manipulativ verbreitete, vorgetäuschte Nachrichten mit der Unterform des „KI-Slop“,⁶⁰ durch betrügerische Schockanrufe oder durch die mit Deepfakes einhergehenden technischen Manipulationen⁶¹, vorgebeugt werden. Entsprechende Transparenzpflichten gelten gemäß Art. 50 Abs. 3 KI-Verordnung schließlich auch für die Betreiber eines Emotionserkennungssystems (Art. 3 Nr. 39 KI-Verordnung) oder eines Systems zur biometrischen Kategorisierung (Art. 3 Nr. 40 KI-Verordnung).

- 59 **Hinweis:** Für die mit solchen Emotionserkennungssystemen oder Systemen zur biometrischen Kategorisierung verbundenen Verarbeitungen personenbezogener Daten verweist Art. 50 Abs. 3 Satz 1 KI-Verordnung betreffend Informationspflichten gegenüber den betroffenen Personen explizit auf die Datenschutz-Grundverordnung – deren Anwendungsbereich ist für sämtliche Verarbeitungen personenbezogener Daten im Zusammenhang mit dem Einsatz von KI-Systemen eröffnet.
- 60 Nach **Art. 50 Abs. 5 KI-Verordnung** müssen die in den vorhergehenden Absätzen genannten Informationen den betreffenden natürlichen Personen spätestens zum **Zeitpunkt** der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt werden und den geltenden Barrierefreiheitsanforderungen entsprechen.
- 61 **Hinweis:** Die Kommission arbeitet derzeit an Leitlinien und einem Verhaltenskodex für transparente KI-Systeme.⁶²
- 62 Verstöße gegen Anforderungen an KI-Systeme mit begrenztem Risiko sind nach **Art. 99 Abs. 4 Buchst. g KI-Verordnung** bußgeldbewehrt.
- 63 **Hinweis:** Die Transparenzpflichten gelten jeweils **nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme, wenn geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen** (vgl. **Art. 50 Abs. 1 Satz 2, Abs. 2 Satz 3, Abs. 3 Satz 2, Abs. 4 UAbs. 1 Satz 2, Abs. 4 UAbs. 2 Satz 2 KI-Verordnung**). In diesen Fällen finden allerdings die datenschutzrechtlichen Vorgaben der **JI-Richtlinie sowie gegebenenfalls die Transparenzpflichten nach der Datenschutz-Grundverordnung** Anwendung.

4. KI-Systeme mit keinem oder geringem Risiko

- 64 KI-Systeme, die keiner der genannten Kategorien zuzuordnen sind, werden als Systeme der Künstlichen Intelligenz mit keinem oder geringem Risiko eingestuft und dürfen nach der KI-

⁶⁰ Unter dem Phänomen des „KI-Slop“ versteht man minderwertige massenhaft durch generative KI-Systeme erzeugte Inhalte wie Texte, Bilder oder Videos, die über soziale Medien und Webseiten verbreitet werden, um schnell Reichweite zu generieren. Unterschieden werden beispielsweise der sogenannte „Berieselungs-Slop“ und der „Rage Slop“. Vgl. hierzu auch den Content-Detektor unter <https://originality.ai/>.

⁶¹ Vgl. hierzu Gesetzentwurf des Bundesrates, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, 5. Juli 2024, erneut eingebracht am 27. August 2025, BR-Drs. 21/1383, auf Gesetzesantrag des Freistaates Bayern vom 14. Mai 2024 hin.

⁶² <https://digital-strategy.ec.europa.eu/en/faqs/guidelines-and-code-practice-transparent-ai-systems> und <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content> m. w. N.

5. Regulierung von KI-Modellen mit allgemeinem Verwendungszweck

Verordnung **frei genutzt** werden. Darunter können beispielsweise Systeme wie KI-fähige Videospiele, Spamfilter oder Empfehlungssysteme, ausweislich EG 54 Satz 5 und 7 KI-Verordnung aber auch bestimmte KI-Systeme für die biometrische Verifizierung fallen.

Die zugrundeliegende **Risikoeinstufung** ist **regelmäßig zu überprüfen**.

65

Hinweis: Auch wenn mit KI-Systemen nach der Einstufung der KI-Verordnung kein oder nur ein geringes Risiko verbunden ist, bedeutet dies nicht, dass eine damit einhergehende Verarbeitung personenbezogener Daten nicht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen im Sinne der Datenschutz-Grundverordnung mit sich bringen kann und dann die dafür dort einschlägigen Vorgaben zu beachten sind.

66

Nach **Art. 95 Abs. 1 KI-Verordnung** soll aufgrund von **Verhaltenskodizes**, einschließlich damit zusammenhängender Governance-Mechanismen, die freiwillige Anwendung einiger oder aller der in Kapitel III Abschnitt 2 KI-Verordnung genannten Anforderungen für Hochrisiko-KI auf KI-Systeme, die kein hohes Risiko bergen, gefördert werden.

67

5. Regulierung von KI-Modellen mit allgemeinem Verwendungszweck (Art. 51 ff. KI-Verordnung)

KI-Systeme, die keinen spezifischen Zweck verfolgen, sondern allgemein zur Text-, Bild-, Video- oder Codegenerierung, Bild- oder Spracherkennung und zu ähnlichen Verwendungszwecken eingesetzt werden können, wie zum Beispiel Große Sprachmodelle, sind sogenannte „KI-Modelle mit allgemeinem Verwendungszweck“ (englisch „general purpose AI [GPAI] systems/models“). Deren Regulierung bildete einen wesentlichen Streitpunkt in den Trilog-Verhandlungen.⁶³

68

Hierunter fallen ausweislich **Art. 3 Nr. 63 KI-Verordnung** KI-Modelle – einschließlich der Fälle, in denen solche KI-Modelle mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert werden –, die eine erhebliche allgemeine Verwendbarkeit aufweisen und in der Lage sind, unabhängig von der Art und Weise ihres Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und die in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden können. Ausgenommen hiervon sind KI-Modelle, die vor ihrer Markteinführung für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen verwendet wurden. KI-Modelle mit allgemeinem Verwendungszweck sind somit zwar wesentliche Komponenten von KI-Systemen, stellen aber für sich genommen keine KI-Systeme dar. Um zu KI-Systemen zu werden, benötigen solche KI-Modelle weitere Komponenten, zum Beispiel eine Benutzeroberfläche (siehe hierzu EG 97 KI-Verordnung). Sobald ein KI-Modell mit allgemeinem Verwendungszweck in ein System integriert ist, wird dieses System als „KI-System mit allgemeinem Verwendungszweck“ angesehen (vgl. Art. 3 Nr. 66 KI-Verordnung).

69

⁶³ Vgl. nur Muller, Stellungnahme für den Bundestagsausschuss für Digitales, 24. Mai 2023, Ausschussdrucksache zu 20(23)158, Internet: <https://www.bundestag.de/resource/blob/984704/cd144349905a80a5dd08db ea1e7f3640/Stellungnahme-Muller-DE.pdf>; Trilog endgültiger Entwurf, 26. Januar 2024, 2021/0106 (COD), S. 5, Internet: <https://artificialintelligenceact.eu/wp-content/uploads/2024/02/AIA-Trilogue-Coreper.pdf>.

III. KI-Verordnung

- 70 **Art. 51 bis Art. 56 KI-Verordnung** enthalten spezifische Regelungen für die Anbieter (nicht jedoch die Betreiber) solcher KI-Modelle mit allgemeinem Verwendungszweck, die **neben dem gestuften, risikobasierten Ansatz** (siehe Rn. 27) stehen. Die Voraussetzungen der Art. 51 ff. (in Verbindung mit EG 97 ff.) KI-Verordnung sind daher im Einzelfall **zusätzlich zu den Vorgaben der für das konkrete KI-System geltenden Risikostufe** zu erfüllen. Zuständig für deren Umsetzung, Beobachtung und Überwachung, unter anderem auf der Grundlage von Praxisleitfäden, ist gemäß Art. 56 in Verbindung mit Art. 3 Nr. 47 KI-Verordnung gegebenenfalls neben⁶⁴ den Mitgliedstaaten insbesondere die Europäische Kommission mit dem **Büro für Künstliche Intelligenz** (hierzu Rn. 84 f.).⁶⁵
- 71 Ziel dieser Regelungen für KI-Modelle mit allgemeinem Verwendungszweck ist es, Transparenz zu gewährleisten und möglichen Risiken von Modellen zu begegnen, die mit einer hohen Leistungsfähigkeit einhergehen. Aus diesem Grund definiert Art. 51 KI-Verordnung für KI-Modelle mit allgemeinem Verwendungszweck **zwei Risikoklassen mit unterschiedlichen Pflichtenkatalogen: Modelle mit „systemischem Risiko“ und „einfache“ Modelle**.
- 72 Ein Modell birgt ausweislich Art. 51 KI-Verordnung systemische Risiken, wenn es eine bestimmte technische Schwelle an Rechenoperationen erreicht (vgl. Art. 51 Abs. 1 Buchst. a KI-Verordnung mit Regelvermutung der „Fähigkeiten mit hohem Wirkungsgrad“ in Art. 51 Abs. 2 KI-Verordnung sowie entsprechende Fähigkeiten oder Wirkung nach Art. 51 Abs. 1 Buchst. b in Verbindung mit Anhang XIII KI-Verordnung) oder vorhersehbare negative Folgen hat (vgl. Art. 52 Abs. 4 UAbs. 1 in Verbindung mit Art. 90 Abs. 1 Buchst. a KI-Verordnung). Über ersteres ist die Kommission unverzüglich vom Anbieter zu informieren (Anmeldepflicht des Art. 52 Abs. 1 KI-Verordnung);⁶⁶ über letzteres entscheidet die Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums gemäß Art. 90 Abs. 1 Buchst. a KI-Verordnung (Art. 52 Abs. 4 UAbs. 1 KI-Verordnung). Gemäß Art. 52 Abs. 6 KI-Verordnung veröffentlicht die Kommission eine Liste von KI-Modellen mit allgemeinem Verwendungszweck, die ein systemisches Risiko begründen.
- 73 Alle KI-Modelle mit allgemeinem Verwendungszweck müssen bestimmten **Transparenzanforderungen** genügen. Dazu gehören nach **Art. 53 KI-Verordnung** die Erstellung einer technischen Dokumentation mit den Angaben nach Anhang XI KI-Verordnung, insbesondere detaillierte **Informationen zu den Trainings-, Test- und Validierungsdaten (Anhang XI**

⁶⁴ Für KI-Systeme, die auf KI-Modellen mit allgemeinem Verwendungszweck beruhen und bei denen das Modell und das System vom selben Anbieter bereitgestellt werden, sollte die Aufsicht – um sich überschneidende Zuständigkeiten zu vermeiden – nach EG 161 Satz 2 KI-Verordnung auf der Unionsebene durch das Büro für Künstliche Intelligenz erfolgen, das für diesen Zweck über die Befugnisse einer Marktüberwachungsbehörde im Sinne der Verordnung (EU) 2019/1020 verfügen sollte.

⁶⁵ Die Europäische Kommission bezeichnet dieses auch als „Europäisches Amt für künstliche Intelligenz“, Internet: <https://digital-strategy.ec.europa.eu/de/policies/ai-office>.

⁶⁶ Nach Art. 52 Abs. 2 KI-Verordnung kann der Anbieter eines KI-Modells mit allgemeinem Verwendungszweck, das die in Art. 51 Abs. 1 Buchst. a KI-Verordnung genannte Bedingung erfüllt, in seiner Mitteilung nach Art. 51 Abs. 1 KI-Verordnung hinreichend begründete Argumente vorbringen, um nachzuweisen, dass das KI-Modell mit allgemeinem Verwendungszweck, obwohl es diese Bedingung erfüllt, aufgrund seiner besonderen Merkmale außerordentlicherweise keine systemischen Risiken birgt und daher nicht als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft werden sollte. Die Kommission kann diese Argumente nach Prüfung zurückweisen, Art. 52 Abs. 3 KI-Verordnung; das KI-Modell mit allgemeinem Verwendungszweck gilt dann als KI-Modell mit allgemeiner Zweckbestimmung mit systemischem Risiko.

Abschnitt 1 Nr. 2 Buchst. c KI-Verordnung), die Einhaltung des EU-Urheberrechts durch Erstellung einer entsprechenden Strategie (Art. 53 Abs. 1 Buchst. c KI-Verordnung) und detaillierter Zusammenfassungen über die für das Training verwendeten Inhalte (Art. 53 Abs. 1 Buchst. d KI-Verordnung) sowie die Kennzeichnungspflicht des **Art. 50 Abs. 1 KI-Verordnung**. Von den Pflichten des Art. 53 Abs. 1 Buchst. a und b KI-Verordnung **ausgenommen** sind gemäß Art. 53 Abs. 2 KI-Verordnung sogenannte **Open Source-Modelle**.

Für **Modelle mit systemischem Risiko** gelten gemäß **Art. 55 KI-Verordnung zusätzliche inhaltliche Anforderungen**: Deren Anbieter müssen Modellevaluierungen durchführen, systemische Risiken bewerten und abschwächen, Gegenteilstests durchführen, der EU-Kommission über schwerwiegende Vorfälle berichten und Cybersicherheit gewährleisten. Bis zur Veröffentlichung harmonisierter EU-Standards sollen die Anbieter hierfür gemäß Art. 56 KI-Verordnung auf Verhaltenskodizes zurückgreifen können, um die Pflichten der KI-Verordnung einzuhalten. 74

Die an KI-Modelle mit allgemeinem Verwendungszweck gestellten Anforderungen müssen nach Art. 113 Abs. 3 Buchst. b KI-Verordnung binnen **zwölf Monaten** nach Inkrafttreten der Verordnung umgesetzt werden. 75

Praxishinweis: Am 10. Juli 2025 hat die Europäische Kommission einen **Praxisleitfaden für KI mit allgemeinem Verwendungszweck** veröffentlicht. Dessen Einhaltung ist bis zur All-gemeingültigerklärung durch die Kommission freiwillig, kann aber zum Nachweis der Konformität mit der KI-Verordnung herangezogen werden, vgl. Art. 53 Abs. 4 Satz 2, Art. 55 Abs. 2 Satz 2 KI-Verordnung. Einige Unternehmen haben den Kodex bereits unterzeichnet und verpflichtet sich damit auch zu regelmäßigen Fortschrittsberichten und zur Zusammenarbeit mit den Aufsichtsbehörden.⁶⁷ Der Leitfaden wird von **Leitlinien zum Umfang der Verpflichtungen für KI-Modelle mit allgemeinem Verwendungszweck**⁶⁸ und der **Vorlage für die öffentliche Zusammenfassung der Schulungsinhalte für KI-Modelle mit allgemeinem Verwendungszweck**⁶⁹ flankiert. 76

6. KI-Kompetenz (Art. 4 KI-Verordnung)

Für **sämtliche Risikostufen** gilt nach Art. 4 KI-Verordnung die generelle Pflicht für Anbieter und Betreiber von KI-Systemen zur Schaffung von „**KI-Kompetenz**“ (englisch „AI literacy“) mit einer Übergangsfrist von nur **sechs Monaten** nach Inkrafttreten der Verordnung ab dem 2. Februar 2025 (Art. 113 Abs. 3 Buchst. a KI-Verordnung). 77

⁶⁷ Zum Ganzen <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>. Kritik hieran äußerte unter anderem eine Koalition von Interessenvertretern aus dem Kultur- und Kreativbereich, Joint statement by a broad coalition of rightsholders active across the EU's cultural and creative sectors, Internet: <https://authorsocieties.eu/content/uploads/2025/07/joint-statement-ai-act-implementation-package-30-july-2025-.pdf>.

⁶⁸ Europäische Kommission, C(2025) 5045 final, 18. Juli 2025, Internet: <https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act>.

⁶⁹ Europäische Kommission, C(2025) 5235 final, 24. Juli 2025, Internet: <https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models>.

III. KI-Verordnung

- 78 Danach müssen Anbieter und Betreiber von KI-Systemen **nach besten Kräften**⁷⁰ sicherstellen, dass ihr **Personal und andere Personen**, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein **ausreichendes Maß** an KI-Kompetenz verfügen. Hierbei sind ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen. Bei „KI-Kompetenz“ in diesem Sinne geht es ausweislich **Art. 3 Nr. 56 und EG 20 KI-Verordnung** um die Fähigkeiten, Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen der KI-Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von Künstlicher Intelligenz und möglicher Schäden, die sie verursachen kann, bewusst zu werden.⁷¹ Besondere Bedeutung kommt KI-Kompetenz dabei ausweislich Art. 26 Abs. 2, EG 91 KI-Verordnung im Hinblick auf Hochrisiko-KI-Systeme zu.
- 79 **Hinweis:** KI-Kompetenz ist auch erforderlich für die datenschutzrechtliche Bewertung der Verarbeitung personenbezogener Daten mittels Künstlicher Intelligenz, beispielsweise im Rahmen des Art. 35 DSGVO.
- 80 Als Umsetzungsmaßnahmen sind unter anderem regelmäßige Schulungen, Informationsmaterial und allgemeine Sensibilisierung jedenfalls⁷² der mit KI-Systemen befassten Beschäftigten denkbar, wobei der Umfang der erforderlichen Kompetenz vom Einzelfall abhängig ist und sich nach dem Grad des Risikos des betreffenden KI-Systems richtet.⁷³ Insofern ist eine **Risikoanalyse** erforderlich (vgl. EG 51 KI-Verordnung). Ein Mangel an KI-Kompetenz kann als

⁷⁰ „Nach besten Kräften“ setzt dabei eine Ergreifung sämtlicher geeigneter und notwendiger Maßnahmen unter Berücksichtigung der konkreten Umstände voraus, vgl. Europäische Kommission, „Best efforts“ Obligation, related provision: Article 8a of Council Regulation 883/2014, Frequently Asked Questions – as of 22 November 2024, Internet: https://finance.ec.europa.eu/document/download/65560de8-a13a-4a58-a87c-ddd27b14e6c1_en?filename=faqs-sanctions-russia-best-efforts-obligation_en.pdf.

⁷¹ Hierzu Cipierre, Konzepte zur Umsetzung der rollen- und kontextspezifischen Anforderungen an die KI-Kompetenz gemäß Art. 4 KI-VO, RDV 2025, S. 26.

⁷² Art. 4 KI-Verordnung könnte auch so verstanden werden, dass die Verpflichtung das gesamte Personal unabhängig von einem konkreten Kontakt mit KI-Systemen umfasst. Mit Blick auf die konkret zu berücksichtigenden Faktoren, insbesondere den Kontext, in dem die KI-Systeme eingesetzt werden sollen, erscheint indes eine Beschränkung auf die mit dem KI-Einsatz befassten Beschäftigten sachgerecht.

⁷³ Europäische Kommission, AI Literacy – Questions & Answers, Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0065>. Die Europäische Kommission identifiziert dabei als Mindestanforderungen: (1) Gewährleistung eines allgemeinen Verständnisses von KI; (2) Berücksichtigung der Rolle der Organisation; (3) Berücksichtigung des Risikos; (4) Konkreter Aufbau von KI-Kompetenzmaßnahmen auf Grundlage der Unterschiede bei den technischen Kenntnissen und des Kontextes. Anregungen für konkrete Umsetzungsmaßnahmen können dem „Living Repository to foster learning and exchange on AI literacy“ (<https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy>) von Mitgliedern des sogenannten KI-Pakts (<https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-Signatories-of-the-AI-Pact>), der KI-Strategie der Europäischen Kommission AI@EC (C[2024] 380 final, 24. Januar 2024, Internet: https://commission.europa.eu/document/download/601a9e64-cdb9-4545-becb-1079ba8c457c_de?filename=DE%20Artificial%20Intelligence%20in%20the%20European%20Commission_0.PDF) sowie der KI-Strategie des EuGH (https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-11/cjeu_ai_strategy.pdf) entnommen werden. Siehe auch Bundesnetzagentur, Hinweispapier KI-Kompetenzen nach Artikel 4 KI-Verordnung, Stand 6/2025, Internet: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/Hinweispapier.pdf.

7. Durchsetzung der KI-Verordnung

Missachtung einer organisationsbezogenen Pflicht angesehen werden, die mittelbar bußgeldrelevante Verstöße nach sich ziehen und von den nationalen Marktüberwachungsbehörden negativ bewertet und/oder sanktioniert werden kann (beispielsweise bei fehlerhafter menschlicher Aufsicht oder Schadensverursachung durch unzureichende Schulungen).⁷⁴

Hinweis: Öffentliche Stellen, die KI-Systeme in eigener Verantwortung einsetzen, können nach der KI-Verordnung als Betreiber oder im Einzelfall sogar als Anbieter von KI-Systemen den eben beschriebenen Handlungspflichten unterworfen sein, insbesondere der für sämtliche Risikoklassen geltenden Pflicht zur Schaffung von KI-Kompetenz eigener Bediensteter und beauftragter Personen. Die insoweit zur Umsetzung ergriffenen Maßnahmen sollten zum Zwecke der Nachweisbarkeit **dokumentiert** werden.

81

Praxishinweis: Im Einzelfall kann auch die Benennung eines KI-Beauftragten als Ansprechpartner und Koordinator für die Kompetenzbildung erwägenswert sein.

82

7. Durchsetzung der KI-Verordnung

Die Umsetzung der KI-Verordnung wird von der Europäischen Kommission zusammen mit den Mitgliedstaaten überwacht.

83

a) Büro für Künstliche Intelligenz (Art. 64 KI-Verordnung)

Die Europäische Kommission ist nach Art. 52, Art. 88 Abs. 1 Satz 1 KI-Verordnung allein zuständige Institution für die **Beaufsichtigung und Durchsetzung der Bestimmungen betreffend KI-Modelle mit allgemeinem Verwendungszweck**.

84

Nach **Art. 88 Abs. 1 Satz 2**, EG 116 ff. **KI-Verordnung** überträgt sie die Durchführung dieser Aufgaben dem **Büro für Künstliche Intelligenz**⁷⁵. Mit Beschluss vom 24. Januar 2024⁷⁶ hat die Europäische Kommission ein Europäisches Amt für künstliche Intelligenz errichtet, das die Funktion dieses in Art. 3 Nr. 47, Art. 64 KI-Verordnung vorgesehenen Büros für Künstliche Intelligenz wahrnehmen soll. Dieses neue Amt ist als Teil der Generaldirektion Kommunikationsnetze, Inhalte und Technologien in die Verwaltung der Kommission integriert. Ihm ist ein

85

⁷⁴ Knappertsbusch/Rappenglück, KI-Kompetenz und verbotene KI-Praktiken als Compliance-Pflicht für Arbeitgeber, CR 2025, S. 281, 282, verorten Art. 4 KI-Verordnung dogmatisch „im Grenzbereich zwischen klassischer Obliegenheit und Schutzpflichtrecht“.

⁷⁵ Die Europäische Kommission bezeichnet dieses auch als „Europäisches Amt für künstliche Intelligenz“, Internet: <https://digital-strategy.ec.europa.eu/de/policies/ai-office>.

⁷⁶ Beschluss der Kommission vom 24. Januar 2024 zur Einrichtung des Europäischen Amts für künstliche Intelligenz, ABl. EU C 2024/1459, S. 1.

III. KI-Verordnung

umfangreicher Aufgabenkreis zugewiesen;⁷⁷ unter anderem hat es ein AI Act Whistleblower Tool zur anonymen Meldung möglicher Verstöße gegen die KI-Verordnung eingerichtet.⁷⁸

b) Behörden in den Mitgliedstaaten

- 86 Parallel dazu müssen die Mitgliedstaaten bis zum 2. August 2025 nach **Art. 28 KI-Verordnung** mindestens eine **notifizierende Behörde** für die Konformitätsbewertungsstellen sowie nach **Art. 74 KI-Verordnung** eine oder mehrere **Marktüberwachungsbehörden** einrichten oder benennen (vgl. Art. 70 Abs. 1 und 2 KI-Verordnung).
- 87 Die Marktüberwachung soll insbesondere gewährleisten, dass Hochrisiko-KI-Systeme den Vorgaben der KI-Verordnung entsprechen. **Die Entscheidung über (eine) deutsche KI-Marktüberwachungsbehörde(n) ist noch nicht getroffen**; ein **Gesetzentwurf der Bundesregierung** vom 10. Februar 2026 sieht in **§ 2 Abs. 1** grundsätzlich eine **zentrale Zuständigkeit der Bundesnetzagentur als KI-Marktüberwachungsbehörde** vor und macht zudem **nicht** von der in **Art. 74 Abs. 8 Satz 1 KI-Verordnung** für KI-Systeme mit hohem Risiko im Bereich der Strafverfolgung, der Grenzverwaltung, der Justiz und der Demokratie im Sinne des Anhangs III Nrn. 1, 6, 7 und 8 KI-Verordnung vorgesehenen Möglichkeit einer **Zuständigkeit der Datenschutzaufsichtsbehörden** als Marktüberwachungsbehörden für diesen Bereich Gebrauch.⁷⁹ Für diese Fälle soll ausweislich § 2 Abs. 5 in Verbindung mit § 4 Entwurf bei der Bundesnetzagentur eine unabhängige KI-Marktüberwachungskammer eingerichtet werden. Ausnahmen von dieser zentralen Zuständigkeitsfestlegung gelten ausweislich § 2 Abs. 2 bis 4 und 8 Entwurf für bestimmte Produktüberwachungsbehörden sowie gemäß **§ 2 Abs. 6 Satz 1 Entwurf** für die Fälle, in denen **öffentliche Stellen der Länder** im Sinne des § 2 Abs. 2 und 3 Bundesdatenschutzgesetz KI-Systeme in Verkehr bringen, in Betrieb nehmen oder verwenden. In Bezug auf Letztere soll die Marktüberwachung den **nach Landesrecht zuständigen Behörden** obliegen.⁸⁰

⁷⁷ Art. 3, 4 Beschluss (Fn. 76). Dazu gehört auch der Austausch mit den freiwilligen Interessenträgern des KI-Pakts, einem Netzwerk zur Unterstützung bei der Umsetzung der KI-Verordnung, vgl. <https://digital-strategy.ec.europa.eu/de/policies/ai-pact> mit einer Übersicht der Unterzeichner und der konkreten Zusagen, sowie der AI Service Desk (<https://ai-act-service-desk.ec.europa.eu/en/ai-act-service-desk>) mit Informationsplattform (<https://ai-act-service-desk.ec.europa.eu/en>).

⁷⁸ <https://digital-strategy.ec.europa.eu/en/policies/ai-act-whistleblower-tool> und <https://ai-act-whistleblower.integrityline.app/>.

⁷⁹ Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (Fn. 53).

⁸⁰ Zur verfassungsrechtlichen Kritik an der vorhergehenden Entwurfsversion, die diese Ausnahme noch nicht enthielt DSK, Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 10. Oktober 2025 zum Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (KI-VO) (Stand 11. September 2025), Internet: https://www.datenschutzkonferenz-online.de/media/st/Stellungnahme_Durchfuehrungsgesetz_KI-VO.pdf unter Verweis auf die föderale Zuständigkeitsordnung nach Art. 30, Art. 83 Grundgesetz. Ebenso Wünschelbaum, Die Zukunft der KI-Regulierung in Deutschland, MMR 2025, S. 259, unter zusätzlichem Hinweis auf die Verschränkung zwischen Art. 74 Abs. 8 und Art. 43 Abs. 1 UAbs. 3 KI-Verordnung. Auch die Digitalministerkonferenz hatte betreffend die Zuständigkeit für Landesbehörden für eine dezentrale Marktüberwachung plädiert, 2. Digitalministerkonferenz, 18. Oktober 2024 in Berlin, TOP 5 „Zusammenwirkungen von Bund und Ländern bei der Durchführung der EU-Verordnung über künstliche Intelligenz“, Internet: https://www.berlin-brandenburg.de/wp-content/uploads/TOP_5_BW_HE_BE_Beschluss_KI-VO.pdf.

7. Durchsetzung der KI-Verordnung

Die Befugnisse der Marktüberwachungsbehörden richten sich ausweislich Art. 74 Abs. 1 KI-Verordnung zunächst nach der **Marktüberwachungsverordnung (EU) 2019/1020**,⁸¹ für die Zwecke der wirksamen Durchsetzung der KI-Verordnung enthält Art. 74 Abs. 2 bis 14 KI-Verordnung Spezifikationen: So verfügen die KI-Marktüberwachungsbehörden insbesondere über – gegebenenfalls Fern- (Art. 74 Abs. 5 KI-Verordnung)⁸² – **Ermittlungsbefugnisse** und können begründete Aufforderungen an Anbieter richten, vgl. Art. 74 Abs. 12 KI-Verordnung. Als ultima ratio können die Marktüberwachungsbehörden nach Art. 74 Abs. 13 KI-Verordnung auch Zugang zum Quellcode eines Hochrisiko-KI-Systems erhalten. 88

Die Marktüberwachungsbehörden erstatten der Kommission und den einschlägigen nationalen Wettbewerbsbehörden gemäß Art. 74 Abs. 2 KI-Verordnung jährlich Bericht über alle im Rahmen der Marktüberwachung ermittelten Informationen, die für die Anwendung des unionsrechtlichen Wettbewerbsrechts von Interesse sein könnten. 89

Anbieter und Betreiber von Künstlicher Intelligenz werden an verschiedenen Stellen der KI-Verordnung dazu verpflichtet, bei den Marktüberwachungsbehörden Meldungen einzureichen oder diesen bestimmte Informationen bereitzustellen. Verstöße gegen diese Anforderungen durch das Unterlassen der Mitteilungen oder durch die Angabe von falschen, unvollständigen oder irreführenden Informationen sind gemäß Art. 99 Abs. 5 KI-Verordnung bußgeldbewehrt. 90

Sind im Rahmen der KI-Verordnung Vorgänge im Zusammenhang mit Hochrisiko-KI-Systemen im Sinne des Anhangs III KI-Verordnung zu bewerten, bei denen die **Datenschutz-Grundrechte berührt** werden, sieht **Art. 77 Abs. 1 Satz 1 KI-Verordnung** eine **Einbindung der nationalen Datenschutzaufsichtsbehörden**⁸³ vor und gestattet ihnen, „sämtliche auf der Grundlage [der KI-Verordnung] in zugänglicher Sprache und Format erstellte oder geführte Dokumentation anzufordern und einzusehen, sofern der Zugang zu dieser Dokumentation für die wirksame Ausübung ihrer Aufträge im Rahmen ihrer Befugnisse innerhalb der Grenzen ihrer Hoheitsgewalt notwendig ist“. Sollte diese Dokumentation nicht ausreichen, kann im begründeten Einzelfall bei der Marktüberwachungsbehörde die Durchführung eines technischen Tests des betreffenden Hochrisiko-KI-Systems beantragt werden, Art. 77 Abs. 3 KI-Verordnung. Eine entsprechende Einbindungspflicht gilt auch für alle anderen nationalen Behörden oder öffentlichen Stellen, die die Einhaltung des Unionsrechts zum Schutz der Grundrechte, einschließlich des Rechts auf Nichtdiskriminierung, in Bezug auf die Verwendung der in Anhang III KI-Verordnung genannten Hochrisiko-KI-Systeme beaufsichtigen oder durchsetzen. 91

Für alle an der Anwendung der KI-Verordnung beteiligten Behörden gelten die Vorgaben zu **Vertraulichkeit, Datenminimierung** („unbedingt erforderlich“) und **Cybersicherheit** nach 92

⁸¹ Verordnung (EU) 2019/1029 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/24/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011, ABl. EU L 169 vom 25. Juni 2019, S. 1.

⁸² Zum Problem der extraterritorialen Wirkung von Hoheitsakten in diesem Zusammenhang Kasper, Die Verwaltung in der KI-Regulierung – Gesichtspunkte bei Betreiben, Nutzen und Beaufsichtigen von KI-Systemen –, DÖV 2025, S. 471, 477.

⁸³ Eine Aufstellung der für den Schutz der Grundrechte zuständigen Behörden im Sinne des Art. 77 KI-Verordnung findet sich unter <https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement>.

III. KI-Verordnung

Art. 78 Abs. 1 und 2 KI-Verordnung. Die Mitgliedstaaten erleichtern die Koordinierung zwischen diesen, Art. 74 Abs. 10 KI-Verordnung.

c) Rechtsdurchsetzung

- 93 Den Marktüberwachungsbehörden stehen die **Abhilfebefugnisse** nach **Art. 79, Art. 80, Art. 82 und Art. 83 KI-Verordnung** zur Verfügung, um auf riskante beziehungsweise nicht konforme KI-Systeme zu reagieren.
- 94 Gemäß **Art. 99 Abs. 1** in Verbindung mit Art. 113 **KI-Verordnung** legen die Mitgliedstaaten bis zum 2. August 2025 die Regeln für **Sanktionen und andere Durchsetzungsmaßnahmen** fest, die bei Verstößen der Marktteilnehmer gegen die KI-Verordnung verhängt werden, und teilen diese der Kommission mit. Mit Blick auf Art. 99 Abs. 8 KI-Verordnung betrifft dies auch die Frage, „in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können“. ⁸⁴
- 95 Im Hinblick auf die **Rechtsdurchsetzung natürlicher Personen** muss die KI-Verordnung im Zusammenhang mit der **überarbeiteten Richtlinie über die Haftung für fehlerhafte Produkte** ⁸⁵ gelesen werden. ⁸⁶
- 96 Diese Richtlinie sieht unter anderem eine verschuldensabhängige Haftung für Schäden vor, die durch KI-Systeme verursacht werden. ⁸⁷
- 97 **Hinweis:** Der **Vorschlag für eine Richtlinie über KI-Haftung** ⁸⁸ wird von der Kommission mangels absehbarer Einigung derzeit nicht weiterverfolgt. ⁸⁹

⁸⁴ Ein vollständiges Absehen von oder auf null reduzierte Geldbußen gegenüber der öffentlichen Hand scheinen daher nicht möglich. Zur nationalen Umsetzung vgl. § 15 Abs. 4 des Gesetzentwurfs der Bundesregierung für ein Gesetz zur Durchführung der Verordnung vom 10. Februar 2026 (Fn. 53).

⁸⁵ Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl. EU L 2024/2853 vom 28. November 2024, S. 1. Bemerkenswert ist insoweit EG 13 Satz 6 Richtlinie (EU) 2024/2853, wonach der Begriff des „Herstellers“ auch Entwickler oder Hersteller von Software, einschließlich der Anbieter von KI-Systemen im Sinne der KI-Verordnung, umfasst. Die nationale Umsetzung muss bis zum 9. Dezember 2026 erfolgen; zum Stand des Gesetzgebungsverfahrens in Deutschland <https://dip.bundestag.de/vorgang/entwurf-eines-gesetzes-zur-modernisierung-des-produkthaftungsrechts/329483>.

⁸⁶ Hierzu Borges, Die Haftung für Software und KI-Systeme nach der neuen Produkthaftungsrichtlinie, CR 2025, S. 1. Allgemein Ringe/Kuhmann, Künstliche Intelligenz und Haftung im Zivilrecht, JZ 2025, S. 227.

⁸⁷ Art. 7 Richtlinie (EU) 2024/2853 enthält dabei Regeln betreffend die „Fehlerhaftigkeit“ und erstreckt sich ausweislich Abs. 2 Buchst. c sogar auf die „Auswirkungen der Fähigkeit des Produkts, nach seinem Inverkehrbringen oder seiner Inbetriebnahme weiter zu lernen oder neue Funktionen zu erwerben“. Die Haftung umfasst mithin auch die genannten Zeiträume und Weiterentwicklungen.

⁸⁸ Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz vom 28. September 2022, COM(2022) 496 final.

⁸⁹ Europäische Kommission, Annexes to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission work programme 2025, Moving forward together: A Bolder, Simpler, Faster Union, 11. Februar 2025, COM(2025) 45 final, Annex IV: Withdrawals No. 32, Internet: <https://commission.europa.eu/document/>

8. Geplante Änderungen der KI-Verordnung

Darüber hinaus kann sich jede natürliche oder juristische Person vor den nationalen Gerichten auf die unmittelbar geltenden Vorschriften der KI-Verordnung berufen und hat nach **Art. 85 Abs. 1 KI-Verordnung** zudem das Recht, sich bei den Marktüberwachungsbehörden zu **beschweren**, wenn sie Grund zu der Annahme hat, dass gegen die Bestimmungen der KI-Verordnung verstoßen wurde. Eine subjektive Rechtsverletzung setzt dieser Rechtsbehelf nicht voraus. Schließlich sind in Bezug auf die KI-Verordnung Verbandsklagen nach der Richtlinie (EU) 2020/1828⁹⁰ möglich.

98

8. Geplante Änderungen der KI-Verordnung

Der Vorschlag für eine **digitale Omnibus-Verordnung über KI**⁹¹ sowie der Vorschlag für eine **Digital-Omnibus-Verordnung**⁹², jeweils vom 19. November 2025, enthalten Änderungsvorschläge der Kommission betreffend die KI-Verordnung sowie die Datenschutz-Grundverordnung, um eine „rechtzeitige, reibungslose und verhältnismäßige Umsetzung bestimmter Bestimmungen des KI-Gesetzes zu gewährleisten“ und um „Unternehmen, öffentlichen Verwaltungen und Bürgern gleichermaßen Soforthilfe zu bieten und die Wettbewerbsfähigkeit zu fördern“. Nach Abschluss der Konsultationsphase⁹³ werden diese dem Europäischen Parlament und dem Rat vorgelegt.

99

download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1__annexes_EN.pdf.

⁹⁰ 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. EU L 409 vom 4. Dezember 2020, S. 1.

⁹¹ Fn. 1.

⁹² Fn. 2.

⁹³ Vgl. hierzu insbesondere EDSA-Europäischer Datenschutzbeauftragter, Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 20. Januar 2026, Internet: https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf, und Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 10. Februar 2026, Internet: https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf. Für weiteren KI-spezifischen Regelungsbedarf in der DSGVO DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Dezember 2025, DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich, Internet: https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_DSGVO_KI_Anpassungen.pdf.

IV. Weitere Vorgaben des Unionsrechts und des nationalen Rechts

1. Unionsrecht

- 100** Neben die Anforderungen der KI-Verordnung treten Vorgaben für Künstliche Intelligenz, die sich aus anderen Normen des **Unionsrechts** ergeben. Die KI-Verordnung stellt insofern keine abschließende Regelung dieser Technologie dar, sondern fügt sich in den bereits bestehenden Rechtsrahmen ein, ohne diesen zu verdrängen.
- 101** Weitere Schutzmechanismen in Bezug auf Künstliche Intelligenz finden sich auf Unionsebene außer in der Datenschutz-Grundverordnung (siehe unten Rn. 114 ff.) insbesondere im Gesetz über digitale Märkte⁹⁴ sowie im Gesetz über digitale Dienste⁹⁵, da es sich bei den insoweit regulierten Systemen auch um KI-Systeme handeln kann.
- 102** Das **Gesetz über digitale Märkte** statuiert Regeln für besonders mächtige Betreiber digitaler Plattformen, die sogenannten „**Torwächter**“⁹⁶ (englisch: „Gatekeeper“): Um Fairness auf den digitalen Märkten als wettbewerbsrechtliches Ziel zu gewährleisten, wird die Marktstellung dieser Torwächter beim Betrieb zentraler Plattformdienste reguliert.
- 103** Das **Gesetz über digitale Dienste** betrifft in erster Linie **Online-Vermittler und Plattformen** wie Online-Marktplätze, soziale Netzwerke, Content-Sharing-Plattformen, App-Stores und Online-Reise- und Online-Unterkunftsplattformen. Es zielt inhaltsbezogen darauf ab, einen sichereren digitalen Raum zu schaffen, in dem die Grundrechte der Nutzer geschützt werden, und gleiche Wettbewerbsbedingungen zu gewährleisten. Dafür enthält das Gesetz allgemeine Vorgaben sowie spezifische Regeln für sehr große Online-Plattformen und Suchmaschinen mit mehr als 45 Millionen Nutzern in der Europäischen Union pro Monat.⁹⁷
- 104** Im Hinblick auf den Zugang zu und die Nutzung von (sowohl personenbezogenen als auch nicht personenbezogenen) Daten können zudem die Vorgaben und der Datenzugangs-

⁹⁴ Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1927 und (EU) 2020/1828, ABl. EU L 265 vom 12. Oktober 2022, S. 1.

⁹⁵ Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2022/31/EG, ABl. EU L 277 vom 27. Oktober 2022, S. 1.

⁹⁶ Von der Kommission bislang als Torwächter benannt sind Alphabet, Amazon, Apple, Booking, ByteDance, Meta und Microsoft (Stand 02/2026), Internet: https://digital-markets-act.ec.europa.eu/gatekeepers_en.

⁹⁷ Hacker, Der AI Act im Spannungsfeld von digitaler und sektoraler Regulierung, Bertelsmann Stiftung, Dezember 2024, S. 20, Internet: https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/AI_Act_im_Spannungsfeld_2024_final.pdf, fordert insoweit eine wechselseitige Berücksichtigung der Verknüpfung von Künstlicher Intelligenz und den systemischen Risiken großer Plattformen.

2. Nationales Recht

anspruch nach der **Datenverordnung**⁹⁸ zu beachten sein, allerdings mit der Einschränkung, dass aggregierte Daten nicht vom Anwendungsbereich umfasst sind.

Ergänzende Anforderungen an die **IT-Sicherheit** mancher KI-Systeme ergeben sich aus der **NIS-2-Richtlinie**⁹⁹, der **Cyberresilienz-Verordnung**¹⁰⁰ sowie im Finanzbereich aus der **Verordnung über die digitale operationale Resilienz im Finanzsektor** (Digital Operational Resilience Act, DORA)¹⁰¹. 105

Schließlich sind generell **sektorspezifische Vorschriften des Unions- beziehungsweise des mitgliedstaatlichen Rechts** zu beachten. 106

Beispiel: Art. 53 Abs. 1 Buchst. e Ziff. ii Verordnung über den europäischen Gesundheitsdatenraum¹⁰² nennt das **KI-Training** ausdrücklich als einen **Zweck, zu dem elektronische Gesundheitsdaten zur Sekundärnutzung** verarbeitet werden können.

2. Nationales Recht

Auf Ebene des **nationalen Rechts** berührt der Einsatz von KI-Systemen ebenfalls weitere Rechtsgebiete, beispielsweise 107

- das Haushaltsrecht,¹⁰³

⁹⁸ Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828, ABl. EU L 2023/2854 vom 22. Dezember 2023, S. 1.

⁹⁹ Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. EU L 333 vom 27. Dezember 2022, S. 80.

¹⁰⁰ Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. EU L 2024/2847 vom 20. November 2024, S. 1.

¹⁰¹ Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. EU L 333 vom 27. Dezember 2023, S. 1. Siehe in diesem Zusammenhang auch Bundesanstalt für Finanzdienstleistungsaufsicht, Orientierungshilfe zu IKT-Risiken beim Einsatz von KI in Finanzunternehmen, Stand 12/2025, Internet: https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/neu/dl_Anlage_orientierungshilfe_IKT_Risiken_bei_KI.pdf.

¹⁰² Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847, ABl. EU L 2025/327 vom 5. März 2025, S. 1.

¹⁰³ Zur Berücksichtigung datenschutzrechtlicher Anforderungen als Kriterium im Vergaberecht siehe Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren, Stand 2/2024, Internet: <https://www.datenschutz-bayern.de/infothek/>. Speziell in Bezug auf die Vorgaben der KI-Verordnung siehe die von der Kommission zur Verfügung gestellten „Standardvertragsklauseln für die Beschaffung von KI-Systemen“, Internet: <https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai>. Hierzu auch Horn/Schuchert, Staatliche Beschaffung von KI-Systemen, MMR 2024, S. 926.

IV. Weitere Vorgaben des Unionsrechts und des nationalen Rechts

- Schutzrechte verschiedener Art (Immaterialgüterrecht,^{104, 105, 106} Schutz vor Diskriminierung,¹⁰⁷ Vertraulichkeitsschutz im weiteren Sinne, Jugendschutzrecht¹⁰⁸) sowie
- das öffentliche Dienst- und das Verwaltungsrecht.

a) Dienstrecht

- 108** Planungen einer öffentlichen Stelle hinsichtlich der Einführung eines KI-Systems können Gegenstand von **Mitwirkungs- oder Mitbestimmungsrechten der Personalvertretung** sein. Je nachdem, in welchem Bereich, zu welchem Zweck und auf welche konkrete Art und Weise ein KI-System eingesetzt werden soll, kann eine Maßnahme der Mitbestimmung (Art. 70 in Verbindung mit Art. 75a Bayerisches Personalvertretungsgesetz - BayPVG) und/oder der Mitwirkung (Art. 72 in Verbindung mit Art. 76 Abs. 1 und 2 BayPVG) der Personalvertretung unterliegen.
- 109** KI-Systeme sollten **nicht zur Leistungskontrolle** der Beschäftigten genutzt werden; auf einen entsprechenden Einsatz muss ausdrücklich hingewiesen werden.

¹⁰⁴ Zu urheberrechtlichen Fragestellungen siehe ausführlich beispielsweise Pech, Urheberrecht trifft Produktsicherheitsrecht: Urheberrechtliche Implikationen der KI-VO – Teil 1, CR 2024, S. 773; Maamar, Urheberrechtliche Fragen beim Einsatz von generativen KI-Systemen, ZUM 2023, S. 481; Baumann, Generative KI und Urheberrecht - Urheber und Anwender im Spannungsfeld, NJW 2023, S. 3673. Vgl. auch Europäisches Parlament, Empfehlungen zum Schutz urheberrechtlich geschützter kreativer Werke vor der Nutzung durch künstliche Intelligenz, 10. März 2026, <https://www.europarl.europa.eu/news/de/press-room/20260306IPR37511/schutz-von-urheberrecht-kreativer-arbeit-im-zeitalter-kunstlicher-intelligenz>. Das LG München I hat im Verfahren der GEMA gegen OpenAI erstmals umfassend zu urheberrechtlichen Fragen in Bezug zu generativer Künstlicher Intelligenz gerichtlich Stellung genommen und stützt sich für weite Teile seiner Argumentation auf eine Memorisierung von Werken im KI-Modell, die als Vervielfältigung angesehen wird, LG München, Urteil vom 11. November 2025, 42 O 14139/24.

¹⁰⁵ Zu patentrechtlichen Fragestellungen allgemein beispielsweise Schröler/Kuß, in: Chibanguza/Kuß/Steeger, Künstliche Intelligenz, 1. Auflage 2022, § 2 E. Rn. 5 ff.; vgl. auch Bundesgerichtshof, Beschluss vom 11. Juni 2024, X ZB 5/22, wonach ein KI-Programm kein Erfinder im Sinne von § 37 Abs. 1 PatG sein kann.

¹⁰⁶ Zum Markenrecht Reich, Haftung für markenrechtsverletzenden Output generativer KI, NJW 2026, 271.

¹⁰⁷ Siehe 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3./4. April 2019 im Hambacher Schloss, Hambacher Erklärung zur Künstlichen Intelligenz, Internet: https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf. Lauscher/Legner, Künstliche Intelligenz und Diskriminierung, ZfDR 2022, S. 367, 371 ff.; Legner, KI-Verordnung und algorithmische Diskriminierung, RD 2024, S. 426; zu „bias“ Shrishak, Bias evaluation, EDSA Support Pool of Experts Programme, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-complex-algorithms-and-effective-data_en. Die gemeinnützige Organisation Algorithm-watch hat unter <https://algorithmwatch.tech/report-algorithmic-discrimination/> die Möglichkeit eröffnet, Fälle zu melden, in denen bei automatisierten oder teilautomatisierten KI-gestützten Entscheidungen der Verdacht einer Benachteiligung im Raum steht.

¹⁰⁸ Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Thema „Generative Künstliche Intelligenz“ vom 22. Mai 2023, S. 6, Internet: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Generative-K%C3%BCnstliche-Intelligenz.pdf; Werry, Generative KI-Modelle im Visier der Datenschutzbehörden, MMR 2023, S. 911, 914.

b) Verwaltungsrecht

Auch im allgemeinen Verwaltungsrecht gibt es Aspekte mit datenschutzrechtlicher Relevanz, die Verantwortliche bei der Nutzung von Künstlicher Intelligenz besonders beachten sollten: 110

Neben dem Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling nach Art. 22 DSGVO (siehe Rn. 239 ff.) stellt insbesondere **§ 10 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern** (AGO) Anforderungen an die **Ablauforganisation von Behörden des Freistaates Bayern**¹⁰⁹ **beim Einsatz der Informations- und Kommunikationstechnik**. Dies umfasst nach **§ 10 Abs. 2 AGO** seitens der jeweiligen Behörde eine **Schulung und Betreuung der Beschäftigten** im erforderlichen Umfang mit Informations- und Kommunikationstechnik. Außerdem gilt für die Beschäftigten, dass **für die Erledigung dienstlicher Aufgaben nur dienstlich bereitgestellte Geräte sowie freigegebene Programme benutzt** werden dürfen (**§ 10 Abs. 4 Satz 1 AGO**). Die Verwirklichung von Vorhaben der Informations- und Kommunikationstechnik der Staatskanzlei und der Geschäftsbereiche erfolgt dabei im Einklang mit den **Standards und Richtlinien für die Informations- und Kommunikationstechnik in der bayerischen Verwaltung** (IKT-Standards-Richtlinien-Bekanntmachung). **Einzelheiten** zum Einsatz und zur Nutzung, der technischen und organisatorischen Gestaltung sowie die erforderlichen Maßnahmen zum Datenschutz und zur Datensicherheit sind **behördenspezifisch** zu regeln (**§ 10 Abs. 5 AGO**). Dies kann beispielsweise in einer internen Richtlinie, Dienstanweisung oder (Rahmen-)Dienstvereinbarung erfolgen, welche je nach Einzelfall Regelungen zu den unter Rn. 374 ff. aufgeführten Inhalten treffen sollte. 111

Die jeweiligen Vorgaben sind durch entsprechende **technische und organisatorische Maßnahmen** zu ergänzen, siehe **§ 10 Abs. 3 AGO** beziehungsweise **Art. 43 Abs. 1 Satz 2 Bay-DiG**. 112

Das Bayerische Digitalgesetz fordert zudem ausdrücklich, den **Einsatz von Künstlicher Intelligenz in der Verwaltung durch geeignete Kontroll- und Rechtsschutzmaßnahmen abzusichern** (**Art. 5 Abs. 2 Satz 2 BayDiG**). Dies können neben den genannten internen Vereinbarungen und Vorgaben insbesondere Maßnahmen zur Sensibilisierung und Schulung der Beschäftigten sein, welche jeweils kontinuierlich überprüft und gegebenenfalls angepasst werden sollten (vgl. hierzu auch die Umsetzungsempfehlungen unter Rn. 366 ff.). 113

¹⁰⁹ Gemeinden, Landkreisen, Bezirken und sonstigen juristischen Personen des öffentlichen Rechts wird nach § 36 AGO empfohlen, ebenfalls nach dieser Geschäftsordnung zu verfahren.

V. Datenschutz-Grundverordnung

- 114 Sowohl für das Training als auch für den Einsatz von KI-Systemen hat neben der KI-Verordnung das Datenschutzrecht eine wesentliche Bedeutung. **Jedes KI-System benötigt große Datensätze**, die – mit Blick auf die oftmals praktizierte Nutzung frei verfügbarer Daten aus dem Internet sowie die allgemeine Häufigkeit des Vorhandenseins in Datensätzen – **in der Regel personenbezogene Daten** enthalten (zum Begriff der personenbezogenen Daten ausführlich unten Rn. 140). Diese Daten können auch zu den in **Art. 9 Abs. 1 und Art. 10 DSGVO** angesprochenen Kategorien zählen (vgl. auch Anhang III KI-Verordnung). Zudem werden KI-Systeme oftmals zur Verarbeitung personenbezogener Daten eingesetzt.
- 115 Diese personenbezogenen Daten stehen auch bei einer Verarbeitung zum Training von oder im Einsatz von KI-Systemen unter dem Schutz der Datenschutz-Grundverordnung, wenn der Anwendungsbereich dieses Gesetzes eröffnet ist.
- 116 Zur Abgrenzung sollten **vier Szenarien** unterschieden werden:
- In Anwendungsszenarien **außerhalb des Geltungsbereichs des Unionsrechts** finden **weder die KI-Verordnung noch die Datenschutz-Grundverordnung, gegebenenfalls aber bereichsspezifisches nationales Recht** Anwendung.
 - Werden **anonyme/anonymisierte** oder **von vornherein nicht personenbezogene** Daten mittels eines KI-Systems im Anwendungsbereich der KI-Verordnung verarbeitet, findet **allein die KI-Verordnung** Anwendung.
 - Ist bei der Verarbeitung personenbezogener Daten **kein KI-System** im Spiel oder eine der **Ausnahmen vom Anwendungsbereich der KI-Verordnung** einschlägig, ist **ausschließlich Datenschutzrecht** (insbesondere die Datenschutz-Grundverordnung) anwendbar.
 - Werden **personenbezogene Daten** zum Training von oder im Einsatz von **KI-Systemen** verarbeitet, sind **sowohl die KI-Verordnung als auch Datenschutzrecht** (insbesondere die Datenschutz-Grundverordnung) zu beachten.
- 117 Damit die Rechte betroffener Personen im letztgenannten Fall angemessen geschützt und die Arbeit mit KI-Systemen überhaupt erst ermöglicht werden können, müssen **datenschutzrechtliche Bestimmungen in jeder Phase des Lebenszyklus' eines KI-Systems** von der Planung und Entwicklung über das Training bis zum Produktivbetrieb **beachtet** werden. Die Dynamik von KI-Systemen erfordert dabei eine kontinuierliche Überprüfung und Anpassung der Datenschutzmaßnahmen, um neuen Entwicklungen und potenziellen Risiken Rechnung zu tragen.
- 118 Bei bayerischen öffentlichen Stellen wird die Einhaltung des Datenschutzrechts (auch) in dieser Konstellation nach Art. 51 f. DSGVO, Art. 15 Bayerisches Datenschutzgesetz (BayDSG) durch den **Bayerischen Landesbeauftragten für den Datenschutz** überwacht. Im Rahmen seiner Zuständigkeiten kann er auf Datenschutzverstöße mit den im Einzelfall zulässigen

1. Verhältnis der Datenschutz-Grundverordnung zur KI-Verordnung

Mitteln (insbesondere auch Maßnahmen nach Art. 58 Abs. 2 und Abs. 6 DSGVO in Verbindung mit Art. 16 BayDSG) reagieren.

1. Verhältnis der Datenschutz-Grundverordnung zur KI-Verordnung

Von wesentlicher Bedeutung für den datenschutzkonformen Betrieb von KI-Systemen, mit denen die Verarbeitung personenbezogener Daten einhergeht, ist daher das **Verhältnis der Vorgaben der Datenschutz-Grundverordnung zu den Regelungen der KI-Verordnung**. 119

a) Allgemeines

Insoweit lässt sich zunächst feststellen, dass KI-Verordnung und Datenschutz-Grundverordnung zwar **Verwandtschaften hinsichtlich ihrer Rechtsgrundlage** (Art. 114 Abs. 1, Art. 16 Abs. 2 Satz 1 Vertrag über die Arbeitsweise der Europäischen Union), der **Anwendung des Marktortprinzips**, des **Grundsatzes der Technologieneutralität** sowie des **risikobasierten Ansatzes** aufweisen. Generell **ergänzt die KI-Verordnung** nach dem Willen des Gesetzgebers **auch die Absicherung der Grundrechte auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten sowie weiterer andere Grundrechte**. 120

Der **Regulierungsansatz** der **Datenschutz-Grundverordnung** ist allerdings **rechtsguts- und verhaltensbezogen**, während die **KI-Verordnung technikbezogene** Regelungen trifft. Inhaltliche Bezugnahmen, auch in Form von Regelungsvorgaben für den jeweils anderen Bereich, finden sich nur punktuell. 121

b) Regelungen der KI-Verordnung im Bereich Datenschutz

So trifft die **KI-Verordnung im Bereich des Datenschutzes** lediglich **vereinzelte eigenständige Regelungen**; im Übrigen nimmt sie die datenschutzrechtlichen Vorgaben in Bezug. Sie stellt insbesondere **grundsätzlich keine Rechtsgrundlagen für Datenverarbeitungen** bereit (vgl. **EG 63 Satz 3 KI-Verordnung**, zu den Ausnahmen siehe Rn. 126). **Art. 2 Abs. 7, EG 9 Satz 2, EG 10 KI-Verordnung** bestimmen, dass die **Vorschriften über den Schutz personenbezogener Daten „unberührt“** bleiben und das Grundrecht auf Schutz personenbezogener Daten insbesondere durch die Datenschutz-Grundverordnung und die JI-Richtlinie geschützt wird (EG 10 KI-Verordnung). 122

KI-spezifische Transparenzpflichten regelt die KI-Verordnung bezogen auf Systeme oder Modelle. Die Transparenzpflichten nach der **Datenschutz-Grundverordnung** werden dadurch nicht ersetzt, sondern **ergänzt**. **Inhaltlich** betreffen die Transparenzpflichten **jeweils unterschiedliche Akteure und unterschiedliche Arten von Informationen**, die für unterschiedliche Adressaten bestimmt sind; Beiträge zu ihrer Erfüllung können gegebenenfalls synergetisch genutzt werden. 123

Beispiel: Die nach Art. 13 KI-Verordnung für die Betreiber bereitzustellenden Informationen können für die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO (hierzu ausdrücklich Art. 26 Abs. 9 KI-Verordnung), für die Information der betroffenen

V. Datenschutz-Grundverordnung

Personen nach Art. 13 f. DSGVO sowie generell für die Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO herangezogen werden

- 124 Ein nach der KI-Verordnung zertifiziertes oder geprüftes System ist nicht automatisch auch datenschutzkonform. Oftmals werden bei einem solchen System aber bereits datenschutzrechtlich relevante Risiken zumindest ein Stück weit reduziert sein.
- 125 **Hinweis:** Eine übergreifende Methodik für das Risikomanagement unter der KI-Verordnung und der Datenschutz-Grundverordnung ist bislang nicht etabliert.
- 126 **Ausnahmsweise gestattet die KI-Verordnung die Verarbeitung von personenbezogenen Daten** durch entsprechende **Rechtsgrundlagen**.
- **Art. 10 Abs. 5 KI-Verordnung** regelt für **Hochrisiko-KI**¹¹⁰ allgemein, dass die Anbieter solcher Systeme in Ausfüllung des Regelungsspielraums des **Art. 9 Abs. 2 Buchst. g, Abs. 4 in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 Buchst. a DSGVO** ausnahmsweise **besondere Kategorien personenbezogener Daten**¹¹¹ **verarbeiten dürfen, soweit dies für die Erkennung und Korrektur von Verzerrungen innerhalb des Hochrisiko-KI-Systems unbedingt erforderlich** ist. Allerdings sind in diesem Fall **angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten** natürlicher Personen zu treffen; das Gesetz legt **zusätzliche Rechtmäßigkeitsbedingungen** fest.
 - Zudem erlaubt **Art. 59 Abs. 1 und 2 KI-Verordnung** in Durchbrechung des Grundsatzes der Zweckbindung unter engen Voraussetzungen als Rechtsvorschrift der Union im Sinne des **Art. 6 Abs. 4 in Verbindung mit**¹¹² **Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 Buchst. a DSGVO** im KI-Reallabor die **Weiterverarbeitung von rechtmäßig für andere Zwecke erhobenen personenbezogenen Daten für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme zur Wahrung eines erheblichen öffentlichen Interesses** (vgl. EG 140 Satz 1 KI-Verordnung).¹¹³ Unberührt hiervon und damit vorrangig anwendbar bleiben allerdings unions- oder nationalrechtliche Regelungen, welche die Verarbeitung personenbezogener Daten für andere Zwecke ausdrücklich ausschließen oder die Datenverarbeitung für die Zwecke der Entwicklung, des Testens oder des Trainings innovativer KI-Systeme festlegen, sowie jegliche andere dem Unionsrecht zum Schutz personenbezogener Daten entsprechende Rechtsgrundlagen (Art. 59 Abs. 3, EG 140 KI-Verordnung).

¹¹⁰ Auf KI-Systeme mit keinem oder geringem Risiko findet diese Ausnahme dagegen keine Anwendung.

¹¹¹ Für eine Ausweitung auf sämtliche personenbezogene Daten Hacker, Der AI Act im Spannungsfeld von digitaler und sektoraler Regulierung (Fn. 97), S. 43.

¹¹² Vergleiche im Einzelnen Buchner/Petri, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 6 DSGVO Rn. 181 ff.

¹¹³ Von der Vorgabe der Entwicklung „zur Wahrung eines erheblichen öffentlichen Interesses“ sind ausweislich Art. 59 Abs. 1 Buchst. a KI-Verordnung die folgenden Bereiche umfasst: öffentliche Sicherheit und öffentliche Gesundheit (i), Aspekte des Umweltschutzes und der Verbesserung der Umweltqualität (ii), nachhaltige Energie (iii), Sicherheit und Widerstandsfähigkeit von Verkehrssystemen, Mobilität, kritischen Infrastrukturen und Netzen sowie Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste (iv).

1. Verhältnis der Datenschutz-Grundverordnung zur KI-Verordnung

Hinweis: Der Begriff des „**KI-Reallabors**“ beschreibt dabei nach **Art. 3 Nr. 55 KI-Verordnung** „einen kontrollierten Rahmen, der von einer zuständigen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter Realbedingungen – zu testen“. Die Mitgliedstaaten sind nach Art. 57 Abs. 1 Satz 1 KI-Verordnung dazu verpflichtet, mindestens ein KI-Reallabor auf nationaler Ebene einzurichten, das bis zum 2. August 2026 einsatzbereit sein muss.¹¹⁴

127

Die mit einem Reallabor einhergehenden (begrenzten) Freiräume zur Erprobung von Innovationen gelten insoweit nicht nur bezüglich des Datenschutzrechts, sondern umfassen alle mit Künstlicher Intelligenz verbundenen Fragestellungen und damit auch Risiken. Der Datenschutz wird dabei im Übrigen nicht außer Kraft gesetzt – **innerhalb des Labors ist insbesondere der Umgang mit personenbezogenen Daten reguliert** (vgl. **Art. 59 Abs. 1 Buchst. b bis i, Abs. 2 und 3 KI-Verordnung**). In der Regel wird insoweit eine vorherige Datenschutz-Folgenabschätzung erforderlich sein.

128

Werden beim Betrieb eines Reallabors personenbezogene Daten verarbeitet, sind die nationalen **Datenschutzbehörden gemäß Art. 57 Abs. 10 KI-Verordnung verpflichtend einzubeziehen**.

129

Hinweis: Soweit (auch) personenbezogene Daten verarbeitet werden, sieht die Datenschutz-Grundverordnung selbst – unabhängig von Künstlicher Intelligenz – in Art. 5 Abs. 1 Buchst. b Halbsatz 2 in Verbindung mit **Art. 89 DSGVO** (sogenanntes **Forschungsprivileg**) als Ausnahme vom Zweckbindungsgrundsatz die Möglichkeit vor, zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken personenbezogene Daten unter bestimmten Voraussetzungen weiterverarbeiten zu dürfen. Dies umfasst auch die Aufsetzung von Reallaboren beziehungsweise „Regulatory Sandboxes“ zu wissenschaftlichen Forschungszwecken.¹¹⁵ Ein besonderer **Fokus** liegt dabei auf der Prüfung der **Erforderlichkeit der Datenverarbeitung**: So genügt es nicht, dass die Verwendung von personenbezogenen Daten das Forschungsziel lediglich begünstigt. Vielmehr muss die Verarbeitung personenbezogener Daten einen Mehrwert für das Forschungsziel mit sich bringen in dem Sinne, dass die Verwendung anonymisierter Daten nicht zielführend ist, da gerade der Personenbezug für die Erreichung des Forschungsziels unerlässlich ist.

130

¹¹⁴ Am 2. Dezember 2025 hat die Kommission den Entwurf eines Durchführungsrechtsaktes zur Einrichtung von KI-Reallaboren nach der KI-Verordnung veröffentlicht, Internet: <https://digital-strategy.ec.europa.eu/en/consultations/commission-seeks-feedback-draft-implementing-act-establish-ai-regulatory-sandboxes-under-ai-act>. Zur Kritik am weiten Gestaltungsspielraum bei der Ausgestaltung der KI-Reallabore und insbesondere der Gefahr des „forum shopping“ vgl. Stroscher/Link, Verarbeitung personenbezogener Daten in KI-Reallaboren nach dem KI-VO-E als Herausforderung für den datenschutzrechtlichen Zweckbindungsgrundsatz, INFORMATIK 2023 - Designing Futures: Zukünfte gestalten, S. 715 ff. m. w. N. Vgl. auch § 13 Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (Fn. 53).

¹¹⁵ Vergleiche hierzu DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. November 2023, Datenschutz in der Forschung durch einheitliche Maßstäbe stärken, Internet: https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliesung_DS.pdf.

V. Datenschutz-Grundverordnung

Als datenschutzrechtliche Rechtsgrundlagen kommen insbesondere Einwilligungen in Betracht. Eine spezialgesetzliche Rechtsgrundlage findet sich beispielsweise im Gesundheitsdatennutzungsgesetz¹¹⁶.

- 131 **Hinweis:** Generell bieten Reallabore einen Rahmen für die (weitere) Entwicklung von zukunftsfähigen Technologien. Das damalige Bundesministerium für Wirtschaft und Energie hat daher bereits im Jahr 2019 ein Handbuch für Reallabore¹¹⁷ und 2021 eine Praxishilfe für den Datenschutz in solchen Laboren¹¹⁸ entwickelt. Derzeit wird auf Bundesebene der Entwurf für ein Reallabore-Gesetz abgestimmt.¹¹⁹
- 132 Für **Tests von Hochrisiko-KI-Systemen unter Realbedingungen** gelten die Vorgaben des **Art. 60 KI-Verordnung**, insbesondere die Informationspflichten gegenüber den zuständigen Marktüberwachungsbehörden. Umfasst ein solcher Test die Verarbeitung personenbezogener Daten, ist insoweit die Datenschutz-Grundverordnung zu beachten, mit der Besonderheit, dass **gemäß Art. 60 Abs. 4 Buchst. i in Verbindung mit Art. 61 KI-Verordnung eine informierte Einwilligung der Testteilnehmer** einzuholen ist und ihre personenbezogenen Daten nach Durchführung der Tests gelöscht werden müssen. Hiervon unberührt bleiben die Anforderungen der Datenschutz-Grundverordnung an die – in einem solchen Fall als eine der datenschutzrechtlichen Rechtsgrundlagen denkbare – Einwilligung in die Verarbeitung personenbezogener Daten nach **Art. 6 Abs. 1 UAbs. 1 Buchst. a in Verbindung mit Art. 4 Nr. 11, Art. 7 DSGVO**; vielmehr stehen die beiden Einwilligungen mit Blick auf deren jeweiligen Pflichteninhalt unabhängig nebeneinander, einzelne Informationen können aber gegebenenfalls synergetisch genutzt werden.

c) Regelungen der Datenschutz-Grundverordnung im Bereich Künstliche Intelligenz

- 133 Die Datenschutz-Grundverordnung enthält ihrerseits keine spezifischen Regelungen für KI-Systeme. Vielmehr wurde sie **nach EG 15 DSGVO bewusst technologieneutral** gefasst und sieht insbesondere keine Ausnahmen und Rahmenbedingungen für die Umsetzung innovativer Technologien vor.

¹¹⁶ Gesetz zur verbesserten Nutzung von Gesundheitsdaten - GDNG, BGBl. 2024 I Nr. 102 vom 25. März 2024. Hierzu Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz und Gesundheitsdatennutzungsgesetz, Orientierungshilfe, Stand 1/2026, Internet: <https://www.datenschutz-bayern.de/infothek/>.

¹¹⁷ Bundesministerium für Wirtschaft und Energie, Freiräume für Innovationen – Das Handbuch für Reallabore, Stand 7/2019, Internet: <https://www.koinno-bmwk.de/koinno/publikationen/detail/freiraeume-fuer-innovationen-das-handbuch-fuer-reallabore/>.

¹¹⁸ Bundesministerium für Wirtschaft und Energie, Praxishilfe zum Datenschutz in Reallaboren, Stand 4/2021, Internet: <https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/praxishilfe-zum-datenschutz-in-reallaboren-1889560>.

¹¹⁹ Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Verbesserung der Rahmenbedingungen für die Erprobung von Innovationen in Reallaboren und zur Förderung des regulatorischen Lernens, Internet: <https://dip.bundestag.de/vorgang/gesetz-zur-verbesserung-der-rahmenbedingungen-f%C3%BCr-die-erprobung-von-innovationen/322128>, mit Etablierung eines Reallabore-Innovationsportals als zentraler Stelle für Beratung, Information, Vernetzung und Wissenstransfer.

1. Verhältnis der Datenschutz-Grundverordnung zur KI-Verordnung

Das heißt, **es gelten die allgemeinen Grundsätze des Datenschutzrechts**: Verarbeitet ein KI-System personenbezogene Daten, sind die Anforderungen der Datenschutz-Grundverordnung, insbesondere das zwingende Erfordernis einer Rechtsgrundlage für die Datenverarbeitung, die Verarbeitungsgrundsätze und die Betroffenenrechte, zu beachten. Der datenschutzrechtlich Verantwortliche muss die Einhaltung der Anforderungen jederzeit nachweisen können (Art. 5 Abs. 2 DSGVO – „**Rechenschaftspflicht**“). Konkretisiert werden diese Vorgaben durch Art. 24 Abs. 1 Satz 1, Art. 25, Art. 32 Abs. 1 DSGVO, wonach unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen durch geeignete technische und organisatorische Maßnahmen sicherzustellen und nachzuweisen ist, dass die Verarbeitung im Einklang mit der Datenschutz-Grundverordnung erfolgt und ein dem Risiko angemessenes Schutzniveau gewährleistet wird. 134

Soweit es um die Verarbeitung personenbezogener Daten geht, stehen die **Interessen der Anbieter und Betreiber von KI-Systemen in einem Spannungsverhältnis zu den Interessen der betroffenen Personen**. Dies wird bereits bei den **Grundsätzen aus Art. 5 Abs. 1 DSGVO** deutlich. So wirken die Grundsätze der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO, Rn. 206 ff.) und der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO, Rn. 211 ff.) dem Bedürfnis entgegen, für das Training und die Verbesserung von KI-Systemen so viele Daten wie möglich zu verwenden. Der Vorteil von Künstlicher Intelligenz, auf der Grundlage eines erheblichen Datenumfangs eigenständig zusätzliche Nutzungsmöglichkeiten zu entdecken und zu entwickeln, muss mit den Grundsätzen der Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO, Rn. 198 ff.) und der Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO, Rn. 197) in Einklang gebracht werden. Zusätzlich kann es bei bestimmten KI-Systemen – mit Blick auf beispielsweise Art. 10 Abs. 3 KI-Verordnung und gerade auch im Hinblick auf die erzielten Ergebnisse – zu Verstößen gegen den Grundsatz der Richtigkeit (Art. 5 Abs. 1 Buchst. d DSGVO, Rn. 208 ff.) und unter Umständen auch zu Diskriminierungen im Widerspruch zum Grundsatz der Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 Buchst. a DSGVO, Rn. 196) kommen. 135

Konkret: Art. 10 Abs. 3 Satz 3 KI-Verordnung schreibt vor, dass die **Trainings-, Validierungs- und Testdatensätze „so weit wie möglich fehlerfrei und vollständig“** sein müssen. Erforderlich ist es daher nach der KI-Verordnung, Daten zu erheben und zu erfassen, die eine sichere und nachvollziehbare Nutzung von KI-Systemen absichern. Dies muss in Einklang gebracht werden mit den Grundsätzen der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) und der Richtigkeit (Art. 5 Abs. 1 Buchst. d DSGVO) sowie den Vorgaben des Datenschutzes durch Technikgestaltung (Art. 25 DSGVO) und der Sicherheit der Verarbeitung (Art. 32 DSGVO), welchen ausweislich Art. 2 Abs. 7 DSGVO Vorrang zukommt. Die genannten Grundsätze stehen allerdings nicht nur in einem Spannungsverhältnis mit Art. 10 Abs. 3, EG 67 KI-Verordnung, sondern können in gewissem Maße auch die Datenqualität steigern. 136

Solche Spannungsverhältnisse erkannte die **Konferenz der unabhängigen Datenschutz-aufsichtsbehörden des Bundes und der Länder** (im Folgenden: DSK) bereits früh und beschloss im **Frühjahr 2019** mit der sogenannten „**Hambacher Erklärung zur Künstlichen Intelligenz**“ **sieben datenschutzrechtliche Anforderungen an Systeme der Künstlichen** 137

V. Datenschutz-Grundverordnung

Intelligenz.¹²⁰ Ein halbes Jahr später folgte die Veröffentlichung eines **Positionspapiers der DSK zu empfohlenen technischen und organisatorischen Maßnahmen** bei der Entwicklung und dem Betrieb von KI-Systemen,¹²¹ welche **Vorgaben und Werkzeuge hierfür in der Datenschutz-Grundverordnung** entwickelt. Dabei sollten die Grundsätze der Datenschutz-Grundverordnung nicht als Innovationshemmnisse, sondern als Unterstützung insbesondere für die Rechtmäßigkeit, Transparenz und Sicherheit von KI-Systemen und damit zur Schaffung von Vertrauen verstanden werden,¹²² während gleichzeitig die konkreten, insbesondere technischen Anforderungen der KI-Verordnung die abstrakten Vorgaben der Datenschutz-Grundverordnung ausfüllen.¹²³

2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Systemen

- 138** Grundsätzlich können (personenbezogene) Daten in unterschiedlicher Form und zu unterschiedlichen Zeitpunkten in KI-Systemen verarbeitet und gegebenenfalls zwischen verschiedenen Verantwortlichen für Komponenten und/oder Lebensphasen übermittelt werden. Mit einem KI-System sind daher regelmäßig verschiedene Datenverarbeitungsvorgänge verbunden.
- 139** **KI-Systeme haben dann datenschutzrechtliche Relevanz, wenn in ihrem Lebenszyklus personenbezogene Daten natürlicher Personen verarbeitet werden, Art. 1 Abs. 1, Art. 2 Abs. 1 DSGVO.**
- 140** Nach **Art. 4 Nr. 1 Halbsatz 1 DSGVO** sind **personenbezogene Daten** „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ beziehen. Ein Personenbezug liegt nicht erst dann vor, wenn sich die Identität einer betroffenen Person unmittelbar aus den verarbeiteten Daten ergibt. Ausreichend ist vielmehr, dass die Informationen eine Identifizierung ermöglichen (Art. 4 Abs. 1 Nr. 1 Halbsatz 2 DSGVO), wobei als mögliche

¹²⁰ DSK, Hambacher Erklärung (Fn. 107):

- „1. KI darf Menschen nicht zum Objekt machen.
2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben.
3. KI muss transparent, nachvollziehbar und erklärbar sein.
4. KI muss Diskriminierungen vermeiden.
5. Für KI gilt der Grundsatz der Datenminimierung.
6. KI braucht Verantwortlichkeit.
7. KI benötigt technische und organisatorische Standards“.

¹²¹ DSK, Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 6. November 2019, Internet: https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf.

¹²² Vgl. Fuchs/Wünschelbaum/Hansen/Walczak, The Bridge Blueprint. Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim KI-Einsatz, öffentlicher Entwurf v.0.9, S. 1, Internet: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/DE-Bridge-Blueprint-v.0.9.pdf.

¹²³ Wünschelbaum, Ein Brückenschlag zwischen DS-GVO und KI-VO: Ein Diskussionsbeitrag zur Überwindung der Rechtsunsicherheit, ZD-Aktuell 2025, 01384.

2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Anwendungen

Identifizierungsmittel insbesondere eine Kennung, eine Kennnummer, Standortdaten, eine Online-Kennung oder eines oder mehrere besondere Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität einer natürlichen Person sind, in Betracht kommen. Ein **Personenbezug** kann **auch durch Kombination mehrerer Informationen** hergestellt werden. Daher schaffen leistungsfähige KI-Systeme regelmäßig, etwa aufgrund – gegebenenfalls zufälliger – Zusammenführung von Daten aus verschiedenen Quellen, besondere Risiken der Identifizierung, bei anonymisierten Daten auch der Re-Identifizierung. Generell misst der Europäische Gerichtshof dem Begriff „personenbezogene Daten“ eine weite Bedeutung zu;¹²⁴ auch sind grundsätzlich¹²⁵ **pseudonymisierte Daten** aufgrund ihrer Personenbeziehbarkeit als personenbezogen anzusehen, Art. 4 Nr. 5, EG 26 Satz 2 DSGVO. Für besondere Kategorien personenbezogener Daten sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gelten nach **Art. 9**¹²⁶ und **Art. 10 DSGVO**¹²⁷ zusätzliche Schutzvorkehrungen.

Mittel, die eine Identifizierung ermöglichen, werden bei Art. 4 Nr. 1 Halbsatz 1 DSGVO allerdings nur so weit berücksichtigt, wie deren **Nutzung hinreichend wahrscheinlich oder vernünftigerweise zu erwarten** ist (vgl. **EG 26 Sätze 3 und 4 DSGVO**).¹²⁸ Dabei sind mit Blick auf EG 26 Satz 3 DSGVO nicht nur die Mittel des Verantwortlichen selbst, sondern auch Erkenntnisse oder Erkenntnismöglichkeiten Dritter zu berücksichtigen. Die Wahrscheinlichkeit einer Nutzung zu Identifizierungszwecken bestimmt sich nach EG 26 Satz 4 DSGVO anhand objektiver Faktoren. Zu berücksichtigen sind dabei in jedem Fall „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen“ (EG 26 Satz 4 am Ende DSGVO). Insoweit kommt der Möglichkeit der (Re-)Identifizierung mittels Künstlicher Intelligenz aufgrund ihrer Leistungsfähigkeit besondere Bedeutung zu; insbesondere können sich vormals anonyme oder als anonymisiert angesehene Daten später als noch oder wieder personenbezogen herausstellen.

141

Solche personenbezogenen Daten werden **verarbeitet** durch „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe [...] wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung, den Abgleich oder die Verknüpfung,

142

¹²⁴ Vgl. nur EuGH, Urteil vom 4. Mai 2023, C-478/21, Rn. 23.

¹²⁵ Zu möglichen Ausnahmen EuGH, Urteil vom 4. September 2025, C-413/23 P (SRB)

¹²⁶ So ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorergehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person nach Art. 9 Abs. 1 DSGVO untersagt, es sei denn, es liegt eine der Ausnahmen des Art. 9 Abs. 2 DSGVO vor.

¹²⁷ Art. 10 Satz 1 DSGVO sieht vor, dass die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen aufgrund von Art. 6 Abs. 1 DSGVO nur unter behördlicher Aufsicht vorgenommen werden darf oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

¹²⁸ EuGH, Urteil vom 9. November 2023, C-319/11, sowie Urteil vom 19. Oktober 2016, C-582/14; zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Wann ist eine natürliche Person identifizierbar?, Aktuelle Kurz-Information 53, Stand 01/2024, Internet: <https://www.datenschutz-bayern.de/infothek/>.

V. Datenschutz-Grundverordnung

die Einschränkung, das Löschen oder die Vernichtung“, **Art. 4 Nr. 2 DSGVO**. Solche Verarbeitungsvorgänge sind in jeder Phase des Lebenszyklus' eines KI-Systems von der Entwicklung über die Implementierung bis zur Nutzung denkbar.

143 Der Einsatz eines KI-Systems entspricht dabei aus datenschutzrechtlicher Sicht oftmals der **Nutzung eines Betriebsmittels**. In diesem Fall ist, wie vor jeder Nutzung eines Betriebsmittels, zu prüfen, ob dessen Einsatz zur Erreichung des jeweiligen Verarbeitungszwecks **erforderlich** ist. Ein KI-System kann dabei nicht nur sachbezogene Daten – also etwa Daten aus dem Fachverfahren, das mit dem Betriebsmittel KI unterstützt wird –, sondern auch seinerseits erhobene „eigene“ personenbezogene Daten verarbeiten, zum Beispiel Anmeldedaten (und damit gegebenenfalls Beschäftigtendaten) oder auch Metadaten wie die IP-Adressen des Betreibers beziehungsweise der einzelnen Nutzer (sogenannte **spezifische Betriebsmitteldaten**).

144 Aus diesem Grund müssen datenschutzrechtlich Verantwortliche schon vorab identifizieren und abgrenzen, welche verschiedenen Verarbeitungen welcher personenbezogenen Daten im Zusammenhang mit einem KI-System stattfinden und wer die jeweils betroffenen Personen sind beziehungsweise sein können. Zudem müssen Verantwortliche prüfen, welche Arten personenbezogener Daten erfasst sind und ob sich daraus oder aus bereichsspezifischen nationalen Regelungen zusätzliche Anforderungen ergeben.

Beispiel: Bereichsspezifische Vorgaben bestehen etwa für Personalaktendaten bei bayerischen Dienstherrn und öffentlichen Arbeitgebern (§ 50 Beamtenstatusgesetz, Art. 103 ff., Art. 145 Bayerisches Beamtengesetz – BayBG) oder Sozialdaten (§§ 67 ff. Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz).

145 Dabei ist zu beachten, dass (besondere Kategorien) **personenbezogene(r) Daten auch erst während einer Verarbeitung entstehen** können, indem mehrere Datensätze miteinander kombiniert werden.

Beispiel: Auf Basis der Anfragen der Nutzer bei einer kommunalen Tourismuswebsite ermittelt ein KI-System für Zwecke der Optimierung der Öffentlichkeitsarbeit die Wahrscheinlichkeit einer sexuellen Orientierung oder religiösen Überzeugung. Für diese Datenverarbeitung müsste dann insbesondere eine Rechtsgrundlage nach Art. 9 Abs. 2 in Verbindung mit Art. 6 Abs. 1 DSGVO vorliegen; auch müsste die Verarbeitung unter Einhaltung der Verarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO erfolgen.

146 Zudem ist zu beachten, ob es sich bei dem genutzten KI-System um ein offenes oder ein abgeschottetes System handelt:

- Bei **abgeschotteten Systemen** erfolgt die Datenverarbeitung in einer eingegrenzten und technisch abgeschlossenen Umgebung. Nur ein eng begrenzter Nutzerkreis hat Zugriff auf das KI-System. Die Kontrolle über die Ein- und Ausgabedaten liegt in abgeschotteten Systemen bei den Nutzern. Bei derartigen KI-Systemen ist oftmals systemseitig nicht vorgesehen, dass die bei der Nutzung eingegebenen oder entstehenden Daten vom Anbieter oder Betreiber des Systems zum weiteren Training verwendet werden, es sei denn, der Betreiber betreibt das System selbst mit eigenen Ressourcen.

2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Anwendungen

- Anders verhält es sich bei **offenen Systemen**: Solche KI-Systeme werden vom Anbieter oder Betreiber zum Beispiel als Cloud-Lösung angeboten und sind in der Regel über das Internet für einen unbestimmten Nutzerkreis zugänglich (KI-as-a-Service). Die Eingabedaten verlassen damit den geschützten Bereich der Nutzer und können, je nach Konzeption des KI-Systems, von diesem auch für die Beantwortung von Anfragen anderer Nutzer verwendet werden. In diesem Fall besteht das Risiko, dass (personenbezogene) Daten ohne Vorliegen einer Rechtsgrundlage nicht nur zum (Weiter-)Training des Systems, sondern auch zu anderen Zwecken weiterverarbeitet werden oder auch unbefugten Dritten zugänglich sind und ihnen gegenüber offengelegt werden. Offene Systeme können überdies Zugang zu weiteren Datenquellen wie dem offenen Internet haben und hierdurch Personenbezug von Daten herstellen oder die Informationen zu einer Person erweitern. Schließlich werden Daten gegebenenfalls auch in Drittstaaten übermittelt, sodass die Vorgaben der Art. 44 ff. DSGVO zu wahren sind.¹²⁹

Einige Anbieter ermöglichen zwar ein Opt-Out bezüglich der Nutzung von Eingabedaten für Trainingszwecke – und bezüglich der Historie, das heißt der Speicherung eines Verlaufs –, hierdurch werden die genannten Probleme aber nicht vollständig gelöst. Abgeschottete Systeme sind daher aus datenschutzrechtlicher Sicht grundsätzlich vorzugswürdig. 147

a) Entwicklung von KI-Systemen

Unter „Entwicklung“ eines KI-Systems wird die Programmierung des zugrundeliegenden KI-Systems beziehungsweise seiner Algorithmen verstanden. Dieser Schritt kommt in der Regel ohne eine Verarbeitung personenbezogener Daten Dritter aus. 148

b) Training von KI-Systemen

Für das anschließende Training des entwickelten Systems, das heißt den Lernprozess einer Künstlichen Intelligenz, werden dagegen oftmals bereits personenbezogene Daten benötigt, die für die unterschiedlichen Phasen des Trainings, nämlich das Initialtraining, das Testen und das Validieren eines KI-Systems, benötigt werden (sogenannte **Trainings-¹³⁰, Test-¹³¹ oder Validierungsdaten¹³²**). 149

Hinweis: Sowohl Programmierung als auch Training können in derselben Hand liegen; es haben sich aber bereits einige Unternehmen auf das Training fremder KI („AI Training-as-a-Service“) spezialisiert. 150

¹²⁹ Siehe hierzu Rn. 358 ff.

¹³⁰ „Trainingsdaten“ werden von Art. 3 Nr. 29 KI-Verordnung definiert als „Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden“.

¹³¹ „Testdaten“ sind nach Art. 3 Nr. 32 KI-Verordnung „Daten, die für eine unabhängige Bewertung des KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen“.

¹³² Der Begriff „Validierungsdaten“ umfasst nach Art. 3 Nr. 30 KI-Verordnung „Daten, die zur Evaluation des trainierten KI-Systems und zur Einstellung seiner nicht erlernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Unter- oder Überanpassung zu vermeiden“.

V. Datenschutz-Grundverordnung

- 151 Beim Training werden mehrere **Techniken des maschinellen Lernens** unterschieden, die grob in „überwachtes Lernen“ (supervised learning) mit der Unterform „bestärkendes Lernen“ (reinforcement learning) und „nicht-überwachtes Lernen“ (unsupervised learning) differenziert werden können und im Einzelfall auch kombiniert sind. Noch in der Entwicklung befindet sich das sogenannte „Causal Machine Learning“ als Begriff für die Verknüpfung von maschinellem Lernen mit der Analyse von Kausalbeziehungen.
- Beim **überwachten Lernen** wird ein KI-System so lange trainiert, bis es die gewünschte Leistungsfähigkeit erreicht hat. Die Ausgabeergebnisse sind daher bereits in der Trainingsphase mehr oder weniger klar.
 - Beim **bestärkenden Lernen** als einer besonderen Form des überwachten Lernens werden in der Trainingsphase die korrekten Ergebnisse nicht vorab zur Verfügung gestellt, jedoch wird jedes Ergebnis dahingehend bewertet, ob es in die „richtige“ oder „falsche“ Richtung geht.
 - Das **nicht-überwachte Lernen** besteht schließlich darin, aus Daten Wissen zu erzeugen: Auf diese Weise trainierte KI-Systeme erkennen Muster und teilen die Daten ohne eine gezielte Vorgabe in Cluster oder Kategorien auf.
- 152 Das Training kann dabei sowohl **zentral** mit einem zentralen Datensatz als auch dezentral (sogenanntes „**Federated Learning**“) ¹³³ durchgeführt werden.
- 153 Im Zusammenhang mit **Großen Sprachmodellen** bedeutet Training zusammengefasst und vereinfacht, dass einer Software mittels eines – in der Regel umfassenden – Datensatzes „beigebracht“ wird, mit welcher statistischen Häufigkeit Worte und Wortteile aufeinanderfolgen. Zukünftige Eingaben sollen dann basierend auf diesem „Wahrscheinlichkeitswissen“ beantwortet werden.
- 154 Das **initiale Training** eines KI-Systems findet vor der Bereitstellung zur Nutzung statt. Manche KI-Systeme werden darüber hinaus während ihres Einsatzes durch die bei Nutzung eingegebenen Daten stetig **weiter- beziehungsweise nachtrainiert**. Außerdem gibt es die Möglichkeit, KI-Systeme durch weiteres Training mit speziellen Inhalten für einen konkreten Einsatz zu spezialisieren (sogenanntes **Fine-Tuning** ¹³⁴).
- 155 In jedem Fall müssen Trainingsdaten erhoben oder zweckgeändert und anschließend für das Training verwendet werden. Diese Daten können nicht nur inhaltlich Personenbezüge aufweisen und im Einzelfall sogar den Kategorien der Art. 9 und 10 DSGVO zuzuordnen sein; es können auch noch personenbezogene Nutzungsdaten der trainierenden Person umfasst sein. Alle diese Daten werden durch die Vorgänge im Rahmen des Trainings verarbeitet.

¹³³ Bei „Federated Learning“ wird ein KI-Modell auf mehreren Geräten trainiert. Jedes teilnehmende Gerät verfügt über einen eigenen lokalen Datensatz, der nicht mit anderen Teilnehmern ausgetauscht wird. Dadurch kann dieser Ansatz Risiken für den Datenschutz minimieren. Zum Ganzen Europäischer Datenschutzbeauftragter, TechDispatch #1/2025 – Federated Learning, 10. Juni 2025, Internet: https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-06-10-techdispatch-12025-federated-learning_en.

¹³⁴ Siehe hierzu unten Rn. 162 ff.

aa) Erhebung von Trainings-, Test- und Validierungsdaten für KI-Systeme

Die Erhebung von Trainings-, Test- und Validierungsdaten durch etwa **Sammeln oder Generieren** von Daten kann sowohl eigenständig als auch durch Rückgriff auf „Drittquellen“ (beispielsweise per Download von Daten aus öffentlich zugänglichen Quellen, insbesondere dem Internet, oder mittels sogenannter „Crawler“¹³⁵ und/oder „Scraping“¹³⁶) erfolgen. Üblich ist auch die Nutzung von lizenzierten Drittquellen, von durch menschliche Trainer generierten Konversationen sowie von Interaktionen zwischen Betreiber beziehungsweise einzelnen Nutzern mit dem System. 156

Diese Daten können Personenbezüge aufweisen.¹³⁷ Mit Blick auf die Vorgaben des Datenschutzrechts sollten die entsprechenden Daten vor Verwendung als Trainings-, Test- und Validierungsdaten idealerweise **anonymisiert**¹³⁸ werden; zumindest sollte die Verarbeitung personenbezogener Daten, beispielsweise durch Pseudonymisierung¹³⁹ oder andere sogenannte „**Privacy Enhancing Technologies**“ wie die Synthetisierung von personen- 157

¹³⁵ Crawling ist der Prozess des automatischen Scannens und Sammelns von Informationen aus Websites im Internet. Ein Website Crawler ist eine automatisierte Software, die zum Navigieren auf Websites, zum Extrahieren und zum Speichern von Daten verwendet wird. Ausgeschlossen sind Websites mit Zugangsbeschränkung in Form eines Anmeldeerfordernisses, Web-Archive sowie Websites des Darknet. Es gibt zudem die Möglichkeit für Betreiber, einen vordefinierten Code auf ihrer Website einzubinden, um zu verhindern, dass die Website von einem Crawler durchsucht wird. Dieser Wunsch wird allerdings nicht immer berücksichtigt.

¹³⁶ Unter Web-Scraping (auch: Data-Scraping) versteht man das automatisierte Extrahieren von Daten auf Websites. Im Gegensatz zum Web-Crawling konzentriert der Web-Scraper sich auf bestimmte Daten, die extrahiert werden sollen, und speichert sie in einem strukturierten Format, zum Beispiel in einer Datenbank oder Tabellenkalkulationsdatei. Einige beliebte Anwendungen von Web-Scraping dienen der Extraktion von Kontaktinformationen, Produktdetails, Bewertungen und Preisvergleichen. Web-Scraping wird häufig von Datenwissenschaftlern und Forschenden verwendet, um große Datenmengen zu sammeln, die für Analysen oder maschinelles Lernen verwendet werden können.

¹³⁷ Speziell zu CommonPool, einer der größten öffentlich zugänglichen Bild-Text-Datensätze aus dem Internet Hong/Hutson/Agnew/Huda/Kohno/Morgenstern, A Common Pool of Privacy Problems: Legal and Technical Lessons from a Large-Scale Web-Scraped Machine Learning Dataset, arXiv:2506.17185, Internet: <https://arxiv.org/abs/2506.17185v1>.

¹³⁸ Mit Blick auf EG 26 DSGVO sind „anonym“ alle Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder ursprünglich personenbezogene Daten, die derart verändert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Für eine wirksame Anonymisierung ist auf den aktuellen Stand der Wissenschaft und Technik abzustellen, der eine (Re-)Identifizierung nach allgemeiner Lebenserfahrung ausschließt oder zumindest einem unverhältnismäßig hohen beziehungsweise unvernünftigen Aufwand unterwirft.

¹³⁹ Pseudonymisierte Daten gelten nach EG 26 Satz 2 DSGVO grundsätzlich als personenbezogene Daten (zu Ausnahmen EuGH, Urteil vom 4. September 2025, C-413/23 P [SRB]). Eine Pseudonymisierung entfaltet allerdings grundsätzlich eine für die Rechte der betroffenen Personen begünstigende Wirkung und kann im Rahmen von Interessenabwägungen Berücksichtigung finden. Vgl. hierzu EDSA, Guidelines 1/2025 on Pseudonymisation, Stand 1/2025, Internet: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en.

V. Datenschutz-Grundverordnung

bezogenen Daten¹⁴⁰, die „Differential Privacy“-Methode¹⁴¹, Deduplikation oder zukünftig gegebenenfalls eine homomorphe Verschlüsselung¹⁴², so weit wie möglich **minimiert** werden.

- 158 **Hinweis:** Diese Vorgänge sind ihrerseits Datenverarbeitungen und bedürfen daher einer Rechtsgrundlage sowie gegebenenfalls einer Zweckänderungsbefugnis.

bb) Aufbereitung von Daten für das Training von KI-Systemen

- 159 Nach der Datenerhebung ist oftmals eine Aufbereitung der Rohdaten in verwendbare Trainings-, Test- und Validierungsdaten erforderlich. Dies geschieht beispielsweise durch Bereinigung und Validierung sowie Strukturierung oder Kategorisierung. Denkbare Maßnahmen sind dabei unter anderem:

- Kuratierung von Quellen und/oder Daten, insbesondere in Form des (vorherigen) Ausschlusses (zum Beispiel von Websites oder Teilen hiervon, deren Quellcode Scraping und/oder der Nutzung für Zwecke der Künstlichen Intelligenz ausdrücklich widerspricht);
- Erkennung und Entfernung von Datensätzen von minderwertiger Qualität durch Filtermethoden mit heuristischen oder klassifikatorengestützten Ansätzen;
- Aufbereitung von besonderen Kategorien personenbezogener Daten durch automatische Entfernung, Kennzeichnung zur Überprüfung durch einen Menschen, Ersetzung oder „Verschleierung“;
- Labeln von Daten, das heißt Anreichern der Daten mit Zusatzinformationen.

cc) Verarbeitung von Daten für das Training von KI-Systemen

- 160 Im Anschluss an diese vorbereitenden Maßnahmen folgt das eigentliche Training, Testen¹⁴³ und die Validierung unter Verwendung der vorbereiteten Trainings-, Test- und Validierungsdaten. Beim Training von KI-Systemen werden die ursprünglich erhobenen oder im Rahmen

¹⁴⁰ Bei synthetischen Daten handelt es sich um ganz oder teilweise künstlich hergestellte Daten, welche die statistischen Merkmale eines realen Datensatzes abstrakt wiedergeben, allerdings keinen Personenbezug aufweisen. Zu Datenschutzmetriken für synthetische Daten vgl. Pilgram et al., A Consensus Privacy Metrics Framework for Synthetic Data, Patterns 2025, Vol. 6 Iss. 10, 101320, Internet: <https://www.sciencedirect.com/science/article/pii/S2666389925001680>. Das alleinige Training mit synthetischen Daten birgt allerdings das Risiko der Erzeugung einer „Echokammer“, Schürmann/Müller-Peltzer, Datenschutzkonforme KI? Anforderungen der Aufsichtsbehörden im Fokus, Datenschutz-Berater 2025, S. 190, 191.

¹⁴¹ „Differential Privacy“ beschreibt eine Anonymisierungstechnik, bei der einem Datensatz zusätzliche Informationen hinzugefügt werden, um eine zufällige Verfälschung der Daten im Sinne eines „technischen Rauschens“ zu erreichen. Hierdurch werden die einzelnen Datenpunkte dergestalt verschleiert beziehungsweise verwischt, dass die statistischen Merkmale eines Datensatzes zwar noch verwertbar bleiben, bestimmte personenbezogene Informationen im Datensatz aber nicht mehr identifiziert werden können.

¹⁴² Mittels der noch in der Entwicklung befindlichen homomorphen Verschlüsselung werden Rechenoperationen an verschlüsselten personenbezogenen Daten durchgeführt und wird relevantes Wissen aus dem jeweiligen Datensatz extrahiert, ohne die personenbezogenen Daten entschlüsseln zu müssen. Auf diese Weise soll datensparsam auf den Informationsgehalt des verschlüsselten Datensatzes zugegriffen werden können.

¹⁴³ Zu den Herausforderungen und möglichen Herangehensweisen beim Testen von KI-Systemen Gautier/Bieringer/Klößner, On the challenges and approaches to test AI systems, DuD 2025, S. 215.

2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Anwendungen

einer Zweckänderung weiterverwendeten Daten als Teil eines Verarbeitungsvorgangs genutzt. Dies umfasst insbesondere Vorgänge wie das **Speichern** der Daten, ihre strukturierte Analyse und **Verwendung** zu Optimierungszwecken sowie ihre Zusammenführung oder **Verknüpfung** mit weiteren Datensätzen, wodurch neue Informationen oder Wahrscheinlichkeitsaussagen generiert werden können. Für Hochrisiko-KI-Systeme sind dabei insbesondere die Vorgaben des Art. 10 KI-Verordnung zu beachten.

Hinweis: Viele KI-Systeme durchlaufen vor ihrem Einsatz zudem eine Phase des sogenannten „**Red-Teaming**“, in der versucht wird, Schwachstellen und Missbrauchsmöglichkeiten zu ermitteln und zu beheben.¹⁴⁴ 161

dd) Fine-Tuning oder Nachtraining von KI-Systemen

In manchen Fällen ist es erforderlich, ein durch einen Dritten vollständig austrainiertes KI-System **vor Nutzung an die jeweiligen internen Maßgaben anzupassen** und ihm beispielsweise beizubringen, (rechtliche) Ausführungen einer bestimmten Behörde auf verständliche Art zu kommunizieren. 162

Diese Konstellationen werden unter dem Begriff des „Fine-Tuning“ oder „Nachtraining“ zusammengefasst und beschreiben die **Aktualisierung und/oder Spezialisierung eines KI-Systems durch weiteres Training mit speziellen Inhalten für einen konkreten Einsatz**. 163

In der Praxis werden hierfür beispielsweise **entweder wiederholt dieselben oder weitere**, insbesondere interne Inhalte wie Vermerke, Schreiben, Bescheide oder sonstige relevante Dokumente importiert, damit das KI-System die Struktur, die Sprache und die Besonderheiten lernt und die ausgegebenen Informationen an diese Vorgaben anpassen kann. 164

Diese Dokumente enthalten oftmals auch personenbezogene Daten. Mit Blick auf die Vorgaben des Datenschutzrechts sollten die entsprechenden Dokumente vor Verwendung als Trainingsdaten idealerweise **anonymisiert, pseudonymisiert** oder es sollte die Verarbeitung personenbezogener Daten zumindest so weit wie möglich **minimiert** werden (siehe hierzu Rn. 206 f.). Dabei ist zu beachten, dass auch Anonymisierung und Pseudonymisierung Verarbeitungsvorgänge darstellen, die Rechtsgrundlagen sowie gegebenenfalls Zweckänderungsbefugnisse benötigen.¹⁴⁵ 165

c) Bereitstellung und Implementierung von KI-Systemen

Systeme der Künstlichen Intelligenz enthalten je nach Training und konkreter Ausgestaltung (beispielsweise als offenes oder abgeschottetes System) zum Zeitpunkt ihrer Bereitstellung durch den Anbieter oder Betreiber und Implementierung durch den Betreiber (gegebenenfalls auch personenbezogene) Daten. Die Implementierung erfolgt dabei in der Regel durch 166

¹⁴⁴ International Working Group on Data Protection in Technology, Working Paper on Large Language Models (LLMs), Stand 12/2024, S. 11, Internet: <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.html>, Red Teaming Artificial Intelligence for Social Good – The PLAYBOOK, Internet: <https://unesdoc.unesco.org/ark:/48223/pf0000394338.locale=en>.

¹⁴⁵ Zu verschiedenen Methoden zur Beseitigung und Beschränkung eines Personenbezugs, siehe Paal, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, ZfDR 2024, S. 129, 135.

V. Datenschutz-Grundverordnung

Installation in der Produktivumgebung des Betreibers einschließlich gegebenenfalls notwendiger Konfigurationen unter Berücksichtigung datenschutzfreundlicher Voreinstellungen („data protection by default“) und der Freigabe für die Nutzung.

- 167 Zur Beantwortung der Frage, ob ein Personenbezug der in einem KI-System enthaltenen Daten vorliegt, ist eine Einzelfallbetrachtung nötig.¹⁴⁶ Dabei sind nicht nur die jeweils zum Einsatz gelangenden **Lernverfahren zu analysieren**, sondern auch die **Wahrscheinlichkeit einer (Re-)Identifizierung** natürlicher Personen **durch atypisches Einwirken auf die Systeme** (sogenannte **Privacy Attacks**, beispielsweise in Form von „Membership Interference Attacks“¹⁴⁷ oder „Model Inversion Attacks“). Ist eine (Re-)Identifizierung **möglich und nach allgemeinem Ermessen wahrscheinlich** (vgl. hierzu EG 26 DSGVO), ist das Vorliegen personenbezogener Daten in dem KI-System zu bejahen.¹⁴⁸ Es bedarf damit grundsätzlich einer **regelmäßigen Risikoüberprüfung**.
- 168 Dabei ist jeweils das **gesamte KI-System zu betrachten**. So könnte zwar argumentiert werden, dass zum Beispiel in dem einem KI-System zugrundeliegenden KI-Modell wie einem (Großen) Sprachmodell keine personenbezogenen Daten gespeichert werden: Technisch wird der Inhalt von (Großen) Sprachmodellen in kleine, vordefinierte Stücke auf der Grundlage numerischer Werte, die sogenannten „Tokens“, geteilt. Diese können aufgrund von bloßen Wahrscheinlichkeiten miteinander in Beziehung gesetzt werden mit der Konsequenz, dass das bloße Vorhalten eines (Großen) Sprachmodells nicht der Datenschutz-Grundverordnung unterläge.¹⁴⁹ Dem lässt sich allerdings entgegenhalten, dass die entsprechenden Wahrscheinlichkeiten zur Funktionsweise der menschlichen Sprache¹⁵⁰ gerade auf

¹⁴⁶ EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, Stand 12/2024, Rn. 34, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de. Bei der Prüfung sollte ausweislich Rn. 38 insbesondere berücksichtigt werden, ob mit vertretbaren Mitteln (i) personenbezogene Daten, die im Zusammenhang mit Trainingsdaten stehen, aus dem Modell extrahiert werden können und ob (ii) die Ausgaben des Modells sich auf die betroffenen Personen beziehen, deren personenbezogene Daten zum Training des Modells verwendet wurden. Zur Anonymisierung vgl. Artikel 29-Datenschutzgruppe, Opinion 05/2014 on Anonymisation Techniques, WP216, Stand 4/2014, Internet: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

¹⁴⁷ EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Fußnoten zu Rn. 38.

¹⁴⁸ Hierzu ausführlich EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 44 ff., mit differenzierender Betrachtung von KI-Modell-Design (Auswahl der Trainingsquellen, Datenaufbereitung und Datenminimierung im Zusammenhang mit dem Training, Methodik des Trainings. Maßnahmen bezüglich der Ausgaben des Modells), KI-Modell-Analyse, KI-Modell-Prüfung und Widerstandsfähigkeit gegen Angriffe sowie Dokumentation, jeweils mit beispielhaften Maßnahmen.

¹⁴⁹ So Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit: Large Language Models und personenbezogene Daten, Diskussionspapier, Stand 7/2024, Internet: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf. Privacy Attacks, die Teile der ursprünglichen personenbezogenen Trainingsdaten zutage fördern, lieferten „bestenfalls zufällige Datenfragmente, eine gezielte Suche nach Informationen über bestimmte Personen im LLM ist nicht möglich“, Fuchs/Wünschelbaum, Wahrscheinlichkeiten reichen nicht: Warum KI-Modelle keine Datenspeicher sind, RDV 2024, S. 314 m. w. N.

¹⁵⁰ Sogenanntes „Natural Language Processing“ (NLP).

2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Anwendungen

Informationen über Umwelt und Menschen und damit auf personenbezogenen Daten beruhen¹⁵¹ – insbesondere fordert die Datenschutz-Grundverordnung kein bestimmtes „Zustandekommen“ des Personenbezugs¹⁵². Zudem können KI-Trainingsdaten durch entsprechendes Prompting in der Ausgabe (weitgehend) unverändert repliziert werden¹⁵³ und ist die Rekonstruktion der beim Training verwendeten Inhalte gerade Sinn und Zwecke insbesondere generativer Künstlicher Intelligenz, da diese doch den Trainingsdaten ähnliche Ausgaben erzeugen soll.¹⁵⁴ Dem steht eine Vereinfachung oder Verkleinerung der Trainingsdaten beispielsweise durch Reduktion oder Entfernung nicht relevanter Inhalte oder Informationen nicht entgegen, ebenso wenig wie die Zerlegung von Daten in Tokens, sofern diese Daten bei Ausgabe wieder zusammengesetzt werden,¹⁵⁵ oder die Bewertung der Replikation als nach dem Nutzungszweck der KI-Modelle unerwünschter Einsatz. Im Übrigen kommen solche KI-Modelle wie (Große) Sprachmodelle nicht isoliert, sondern nur als Teil eines KI-Systems mit Benutzerschnittstelle und beispielsweise Eingangs- und Ausgangsfilter zum Einsatz. In diesem Rahmen finden – beispielsweise durch Ein- oder Ausgabe personenbezogener Daten –

¹⁵¹ Schwartmann/Köhler, Warum es auf Wahrscheinlichkeiten ankommt: Darum sind personenbezogene Daten auch in LLM geschützt, RDV 2024, S. 316: „Die Eigenheiten der menschlichen Sprache führen [...] regelmäßig dazu, dass eine wahrscheinliche Wortfolge eine bestimmte Information über eine Person vermittelt.“

¹⁵² Schwartmann/Köhler, Warum es auf Wahrscheinlichkeiten ankommt: Darum sind personenbezogene Daten auch in LLM geschützt, RDV 2024, S. 316; Hansen/Walczak, KIR 2024, S.82, 84; Nolte/Finck/Meding, Machine Learners Should Acknowledge the Legal Implications of Large Language Models as Personal Data, arXiv:2025.01630, Internet: <https://arxiv.org/abs/2503.01630>.

¹⁵³ Nasr et al., Extracting Data from ChatGPT, 11/2023, Internet: <https://not-just-memorization.github.io/extracting-training-data-from-chatgpt.html> und <https://spylab.ai/blog/training-data-extraction/>. Cooper/Grimmelmann, The Files are in the Computer: On Copyright, Memorization, and Generative AI, Internet: <https://james.grimmelmann.net/files/articles/the-files-are-in-the-computer.pdf>, S. 23 f. „A model is not a magical portal that pulls fresh information from some parallel universe into our own. A model is a data structure: it consists of information derived from its training data. The memorized training data are in the model.“ In diesem Sinne auch EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 31.

¹⁵⁴ Zu dem in diesem Zusammenhang relevanten Phänomen des „Ambiguitätskollaps“ beziehungsweise „Mehrdeutigkeitskollaps“ Gur-Arieh/Wang/Fazelpour, Ambiguity Collapse by LLMs: A Taxonomy of Epistemic Risks, arXiv:2026.05801, Internet: <https://arxiv.org/abs/2603.05801>. Dabei geht es um Einschränkungen, die prädiktive Große Sprachmodelle bei der Interpretation komplexer Textinformationen mit sich bringen, sowie mögliche Abschwächungsmaßnahmen. So neigten LLM in Situationen, in denen sie zwischen Schlussketten wählen müssen, die sich auf ein Wort-Token beziehen und in verschiedenen Kontexten mehrere Bedeutungen haben können dazu, die meisten Bedeutungen abzutun, die für ein Wort wirklich relevant seien.

¹⁵⁵ Vgl. EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 31: „Nach Ansicht des EDSA kann es, selbst wenn ein KI-Modell nicht absichtlich darauf ausgelegt wurde, Informationen aus den Trainingsdaten auszugeben, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, doch vorkommen, dass Daten aus dem Trainingsdatensatz – einschließlich personenbezogener Daten – nach wie vor in den Parametern des Modells „absorbiert“ (d. h. durch mathematische Objekte repräsentiert) sind. Es mag sein, dass diese Daten sich von den ursprünglichen Trainingsdatenpunkten unterscheiden, aber dennoch weiterhin die ursprünglichen Informationen dieser Daten enthalten, die dann möglicherweise letztendlich direkt oder indirekt aus dem Modell entnommen oder in sonstiger Weise daraus erlangt werden können. Soweit es möglich ist, mit Mitteln, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, aus einem KI-Modell Informationen zu erlangen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, deren personenbezogene Daten für das Training eines Modells verwendet wurden, lässt dies den Schluss zu, dass ein derartiges Modell nicht anonym ist“.

V. Datenschutz-Grundverordnung

regelmäßig Verarbeitungen von Daten mit Personenbezug statt, sodass von einem Personenbezug des gesamten KI-Systems einschließlich des zugrundeliegenden KI-Modells auszugehen ist und dieses Gesamtsystem der datenschutzrechtlichen Bewertung unterliegt.

- 169 Soweit das **Training vor Anschaffung beziehungsweise Nutzung eines KI-Systems bereits abgeschlossen** ist, hat die einsetzende Stelle auf einen etwaigen Personenbezug der Trainingsdaten zwar keinen Einfluss; sie muss dies aber im Zusammenhang mit der (weiteren) Nutzung bedenken: Als datenschutzrechtlich Verantwortlicher für ein von ihr als Betriebsmittel eingesetztes KI-System muss sie dessen datenschutzkonforme Nutzung sicherstellen und nachweisen (Art. 5 Abs. 2 DSGVO). Dies umfasst **auf der Grundlage einer Einzelfallbetrachtung auch die Frage der Rechtmäßigkeit des vorhergehenden Trainings und dessen Auswirkungen auf die Rechtmäßigkeit der Nutzung** des betreffenden Systems; den Verantwortlichen trifft insoweit eine bezüglich des Umfangs einzelfallspezifische aufsichtsbehördlich überprüfbare **Pflicht zur „angemessenen Bewertung“**¹⁵⁶ sowie gegebenenfalls auch zur (Prüfung der) Umsetzung sogenannter **„risikomindernder Maßnahmen“**¹⁵⁷. Die einsetzende Stelle ist zudem insbesondere zur Gewährleistung der Transparenzpflichten (Art. 12 ff. DSGVO, hierzu Rn. 296 ff.) und Betroffenenrechte (Art. 15 ff. DSGVO, hierzu Rn. 310 ff.) verpflichtet.
- 170 Die **Bereitstellung** eines KI-Systems zur Nutzung sowie seine **Implementierung** stellen dabei – Personenbezug vorausgesetzt – **separate Verarbeitungsvorgänge** dar: Zum einen die Bereitstellung des Personenbezug aufweisenden KI-Systems vom Anbieter an den Betreiber als Verarbeitungsvorgang „Bereitstellung personenbezogener Daten“. Zum anderen die Implementierung des Personenbezug aufweisenden KI-Systems durch Installation und gegebenenfalls Konfiguration in der Produktivumgebung des Betreibers, das heißt Verarbeitungsvorgang „Verknüpfung personenbezogener Daten“.

¹⁵⁶ EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 122, 126, 128 ff. Die Aufsichtsbehörden sollten dabei unter anderem berücksichtigen, ob der Verantwortliche beispielsweise die Datenquelle und einen möglichen (gegebenenfalls aufsichtsbehördlich oder gerichtlich festgestellten) Verstoß des KI-Modells gegen die Datenschutz-Grundverordnung bewertet hat, Rn. 129 f. Der Grad der Bewertung des Verantwortlichen und der von den Aufsichtsbehörden erwartete Detaillierungsgrad können dabei in Abhängigkeit von verschiedenen Faktoren variieren, einschließlich der Art und des Ausmaßes der Risiken, die durch die Verarbeitung im KI-Modell während seines Einsatzes in Bezug auf die betroffenen Personen, deren Daten zur Entwicklung des Modells verwendet wurden, entstehen, Rn. 130. Der Verantwortliche darf sich in jedem Fall nicht ausschließlich auf eine Konformitätserklärung des KI-Anbieters nach Art. 16 Buchst. g, Art. 47 KI-Verordnung stützen, Rn. 131. Nach Auffassung von Keber/List, Die datenschutzrechtliche Zulässigkeit des Einsatzes von KI-Modellen, DuD 2025, S. 284, 287, liegt eine offensichtliche beziehungsweise leicht erkennbare Rechtswidrigkeit eines KI-Modells jedenfalls dann nahe, wenn der einsetzende Betreiber über dessen Trainingsdaten keinerlei Informationen hat und sich um ihren Erhalt im Rahmen des Zumutbaren auch nicht bemüht.

¹⁵⁷ Hierzu EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 132 in Verbindung mit Rn. 96 ff. Zu möglichen risikomindernden Maßnahmen im Zusammenhang mit Großen Sprachmodellen Barberá, AI Privacy Risks & Mitigations – Large Language Models (LLMs) (Fn. 12).

d) Nutzung von KI-Systemen

Als Nutzer von KI-Systemen in der öffentlichen Verwaltung kommen, je nach Einsatzszenario, nicht nur Beschäftigte der ein KI-System betreibenden bayerischen öffentlichen Stellen, sondern auch Bürgerinnen und Bürger in Betracht. Differenziert werden können insbesondere die nachfolgend näher erläuterten Verarbeitungsvorgänge. Weiterhin wird auf die Ausführungen zum Fine-Tuning unter Rn. 162 ff. verwiesen, da dieses auch häufig im Rahmen der Nutzung von KI-Systemen stattfindet. 171

Beispiele: Eine bayerische öffentliche Stelle ermöglicht ihren Beschäftigten die Nutzung eines anmeldepflichtigen Großen Sprachmodells. – Bürgerinnen und Bürger interagieren mit einem KI-betriebenen Chatbot auf der Website einer öffentlichen Stelle.

aa) Eingabe (personenbezogener) Daten des Nutzers bei der Anmeldung bei einem KI-System

Manche KI-Systeme sind nur nach **Anmeldung mit einem personen- oder zumindest organisationsbezogenen Login** nutzbar. 172

Um insoweit eine Verarbeitung personenbezogener Daten einzelner Nutzer zu vermeiden oder zumindest zu beschränken, wird eine jedenfalls pseudonymisierte Nutzung über Login-Daten ohne Namensnennung empfohlen, die – soweit zulässig – gegebenenfalls von einer ganzen Organisationseinheit genutzt werden können (**Funktionsaccounts**). Zudem ist bei bayerischen öffentlichen Stellen für die Erledigung dienstlicher Aufgaben ein Einsatz nur über dienstliche Geräte zuzulassen (vgl. **§ 10 Abs. 4 AGO in Verbindung mit § 36 AGO**). 173

Beispiel: Eine Behörde möchte ihren Beschäftigten die Nutzung eines anmeldepflichtigen Großen Sprachmodells gestatten. Zur Minimierung der Verarbeitung der Nutzerdaten in Gestalt sowohl der Anmeldedaten als auch der nutzerbezogenen Betriebsmitteldaten will die Behörde einen Drittanbieter einsetzen, der damit wirbt, die Nutzung des Großen Sprachmodells über eine von ihm angebotene Schnittstelle anonym zu ermöglichen.

In diesem Beispiel muss die Behörde neben den allgemeinen (datenschutz-)rechtlichen Verpflichtungen im Zusammenhang mit dem Drittanbieter überprüfen, inwieweit tatsächlich eine anonyme Nutzung des Großen Sprachmodells vermittelt wird, oder ob die Nutzerdaten möglicherweise nur pseudonymisiert übermittelt werden.

Hinweis: OpenAI bietet seit dem 1. April 2024 schrittweise weltweit eine anmeldefreie Version des Großen Sprachmodells ChatGPT mit eingeschränkten Funktionalitäten an, sogenanntes „Signed Out ChatGPT“. ¹⁵⁸ Es kann – je nach Nutzereinstellungen – ein Weitertraining mit den eingegebenen Daten erfolgen. Zudem werden aggregierte Nutzungsdaten und Geräteinformationen erhoben und verarbeitet, es wird eine Historie erstellt (die jedoch nicht einsehbar ist) und eine strengere Inhaltsmoderation als bei eingeloggten Nutzern vorgenommen. 174

¹⁵⁸ Internet: <https://openai.com/index/start-using-chatgpt-instantly/>.

bb) Eingabe (personenbezogener Daten) bei der Nutzung eines KI-Systems

- 175 Auch die **Arbeitsanweisung oder Aufforderung**, die der Nutzer einem KI-System gibt (bei generativer Künstlicher Intelligenz als „**Prompt**“ bezeichnet¹⁵⁹), kann personenbezogene Daten enthalten.

Beispiele für Prompts für generative KI-Systeme wie Große Sprachmodelle: „Erstelle eine Zusammenfassung der Anfragen von Frau Meier.“ – „Verfasse eine Eingangsbestätigung an Herrn Müller zu dessen Schreiben vom 5. April.“

cc) Verarbeitung der eingegebenen Daten mit innerhalb eines KI-Systems vorhandenen Daten

- 176 Für die Ausführung einer Arbeitsanweisung werden oftmals personenbezogene Daten verarbeitet, gegebenenfalls unter **Verknüpfung mit den bereits (aufgrund des Trainings) innerhalb des KI-Systems vorhandenen (personenbezogenen) Daten**.

Beispiele: Abgleich von genetischen Datensätzen zur Diagnose von Krankheiten; Abfrage von genetischen Datensätzen, die bestimmte Merkmale aufweisen; Abfassung eines Glückwunschschreibens mit Würdigung der Lebensleistung.

- 177 Ob und, wenn ja, inwieweit die Verarbeitung der eingegebenen Daten mit innerhalb eines KI-Systems vorhandenen Daten datenschutzrechtlich zulässig sein kann, hat die einsetzende Stelle zu klären. Grundsätzlich ist es ratsam, – soweit möglich – nur anonyme Daten einzugeben.
- 178 Im Zusammenhang mit der Nutzung von **(Großen) Sprachmodellen** ist dabei die Technik der „**Retrieval Augmented Generation**“ (RAG) zu berücksichtigen:¹⁶⁰ So nutzen KI-Sprachmodelle beim Beantworten von Prompts grundsätzlich nur die Daten und Dokumente, mit denen sie trainiert wurden. Mit RAG werden diese KI-Sprachmodelle in die Lage versetzt, **weitere (außerhalb des [Großen] Sprachmodells liegende) Datenquellen wie Dokumentensammlungen, Datenbanken oder einen Knowledge Graph heranzuziehen** (sogenanntes **RAG-Subsystem**). Dabei werden diese Referenzdokumente zunächst aufbereitet, beispielsweise durch Aufteilung in kürzere Absätze (Chunks), Überführung in Vektoren mittels eines KI-Embedding-Modells¹⁶¹ und Speicherung in einer Vektordatenbank¹⁶². Wann immer Nutzer dann Arbeitsanweisungen geben, wird die Anfrage mittels des Embedding-Modells wiederum in einen Anfragevektor überführt und an den sogenannten Retriever

¹⁵⁹ Zu verschiedenen Prompt-Techniken vgl. International Working Group on Data Protection in Technology, Working Paper on Large Language Models (LLMs) (Fn. 143), S. 26 f. m. w. N.

¹⁶⁰ Zum Ganzen DSK, Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode, Version 1.0, Stand 10/2025, Internet: https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf.

¹⁶¹ Zur Bedeutung der Wahl des Embedding-Modells, insbesondere hinsichtlich des sprachlichen Kontexts, Gerst, RAG mit deutschsprachigen Embedding-Modellen, iX 2/2025, S. 143 ff.

¹⁶² Die Vektoren sind numerische Darstellungen der Textdaten, welche die semantische Bedeutung des Textes erfassen und einen Ähnlichkeitsvergleich ermöglichen.

2. Datenverarbeitungsvorgänge im Zusammenhang mit KI-Anwendungen

übergeben, der die Vektordatenbank nach denjenigen Vektoren durchsucht, welche eine möglichst geringe Distanz (d.h. große semantische Nähe) zum Anfragevektor haben. Anschließend wird die Eingabe des Nutzers um das Suchergebnis des Retrievers ergänzt, bevor sie an ein Sprachmodell weitergegeben wird, welches – im derzeit technisch noch nicht erreichbaren Idealfall¹⁶³ – nur diese relevanten Inhalte für die Beantwortung als Kontext nutzen soll (sogenanntes **RAG-System**). Durch den Einsatz von RAG können unter anderem behördeninterne Dokumente und Informationen einfacher zugänglich gemacht werden.

RAG **unterscheidet sich dabei vom Fine-Tuning** dahingehend, dass sie einen unmittelbaren Zugang zu variablen (externen) Datenquellen ermöglicht, ohne diese in das KI-System selbst zu integrieren. Eine solche Integration spezifischer Datensätze ist durch Fine-Tuning zwar möglich; allerdings können die betreffenden Daten nur durch ein zeitaufwendiges (erneutes) Training in das KI-System eingefügt werden, und jede Aktualisierung erfordert einen neuen Trainingszyklus. Zudem sind nicht alle Datensätze für ein Fine-Tuning geeignet; die Qualität der Ergebnisse variiert entsprechend den (zugrunde liegenden) Datensätzen.

179

Hinweise: Enthalten die **mittels RAG eingebundenen Datenquellen personenbezogene Daten**, findet auch auf diese hinsichtlich sowohl der im RAG-Subsystem (zum Beispiel Erhebung der Referenzdokumente, Aufbereitung der Referenzdokumente und Vektorisierung) als auch im RAG-System insgesamt (zum Beispiel Verarbeitung mittels des [Großen] Sprachmodells, Ausgabe durch das [Große] Sprachmodell) erfolgenden Datenverarbeitungen das Datenschutzrecht Anwendung. Für das **KI-gestützte Embedding-Verfahren**, bei dem zunehmend (Große) Sprachmodelle zum Einsatz kommen, gelten sämtliche Ausführungen in dieser Orientierungshilfe entsprechend; dabei sind auch mögliche Angriffe und daraus folgend (unberechtigte) Zugriffe auf oder Rekonstruktionen aus der Vektordatenbank zu berücksichtigen.¹⁶⁴

180

Der Einsatz von RAG kann in datenschutzrechtlicher Hinsicht aber auch **gewisse Erleichterungen** mit sich bringen: Da in einem RAG-System die Inhalte wesentlich über das RAG-Subsystem gesteuert werden sollen und das im KI-System implementierte Sprachmodell (vorrangig) nur zur Textgenerierung verwendet werden soll, ist es im Einzelfall auch möglich, ein RAG-Subsystem (mit gegebenenfalls personenbezogenen Datenquellen) an ein KI-System mit Sprachmodell ohne Personenbezug beziehungsweise mit anonymisiertem Sprachmodell anzubinden. Gewährleistung und Umsetzung der Informationspflichten und Betroffenenrechte sowie Einhaltung der Verarbeitungsgrundsätze insbesondere der Richtigkeit der Daten, ihrer Integrität und Vertraulichkeit sowie der Datenminimierung und Speicherbegrenzung können in Bezug auf die mittels RAG angeschlossenen externen Datenquellen durch den insoweit Verantwortlichen – beispielsweise die einsetzende öffentliche Stelle – gesteuert oder zumindest beeinflusst werden können. Herausforderungen – und gegebenenfalls

¹⁶³ Wu/Wu/Zou, ClashEval: Quantifying the tug-of-war between an LLM's internal prior and external evidence, 38th Conference on Neural Information Processing Systems (NeurIPS 2024) Track on Datasets and Benchmarks, Internet: https://proceedings.neurips.cc/paper_files/paper/2024/file/3aa291abc426d7a29fb08418c1244177-Paper-Datasets_and_Benchmarks_Track.pdf. Im Gegenteil haben Untersuchungen gezeigt, dass mittels Retriever ergänzter Kontext, welcher stark vom antrainierten Wissen des eingesetzten Sprachmodells abweicht, weniger wahrscheinlich für Antworten in Betracht gezogen wird (sogenannter Context-Bias).

¹⁶⁴ Morris/Kuleshov/Shmatikov/Rush, Text Embeddings Reveal (Almost) As Much as Text, arXiv:2310.06816, Internet: <https://arxiv.org/abs/2310.06816>.

(vertraglich abzusichernder) Unterstützungsbedarf durch den Anbieter des jeweiligen KI-Systems/KI-Modells (hier: zumindest KI-Embedding-Modell, KI-System mit Sprachmodell) – bestehen dagegen weiterhin insbesondere hinsichtlich der Gewährleistung der Informationspflichten und Betroffenenrechte im Hinblick auf das RAG-System und die dort zum Einsatz kommenden KI-Modelle insgesamt sowie in Bezug auf die Grundsätze der Rechtmäßigkeit, Transparenz und Zweckbindung.¹⁶⁵ In die datenschutzrechtliche Bewertung muss zudem mit einbezogen werden, dass bei einem RAG-System mit dem Embedding-Modell im RAG-Subsystem mindestens ein weiteres KI-Modell zum Einsatz kommt.

dd) Verarbeitung von spezifischen Betriebsmitteldaten beim Einsatz eines KI-Systems

- 181** Wie gesehen entspricht der Einsatz eines KI-Systems oftmals der Nutzung eines Betriebsmittels. Mithin ist wie vor der Nutzung jedes Betriebsmittels zu prüfen, ob dessen **Einsatz zur Erreichung des jeweiligen Verarbeitungszwecks erforderlich** ist. Diese Prüfung erfolgt gegebenenfalls im Rahmen einer Datenschutz-Folgenabschätzung (siehe dazu Rn. 349 ff.).
- 182** Beim Einsatz eines KI-Systems sind Verarbeitungen unterschiedlicher Kategorien personenbezogener Daten zu unterscheiden: Zum einen verarbeitet das KI-System die im Rahmen seiner zweckgemäßen Nutzung anfallenden Inhaltsdaten, insbesondere solche Daten, die der Erfüllung der durch den Einsatz des KI-Systems unterstützten Aufgaben dienen. Zum anderen verarbeitet das KI-System eigenständig erhobene personenbezogene Daten, die nicht unmittelbar der Aufgabenerfüllung zuzurechnen sind. Hierzu zählen insbesondere Authentifizierungs- und Anmeldedaten (einschließlich gegebenenfalls betroffener Beschäftigtendaten) sowie technische Metadaten wie IP-Adressen der einzelnen Nutzer. Diese Daten werden als **spezifische Betriebsmitteldaten** verarbeitet.
- 183** Nutzer eines von einer öffentlichen Stelle betriebenen KI-Systems, deren spezifische Betriebsmitteldaten durch das System verarbeitet werden, können dabei, je nach Einsatzszenario, Beschäftigte dieser bayerischen öffentlichen Stelle, aber auch Bürger sein, die einen KI-betriebenen öffentlichen Dienst wie beispielsweise einen Chatbot in Anspruch nehmen. Auch in Bezug auf diese Datenverarbeitungen sind die Grundsätze des Datenschutzrechts zu wahren.
- 184** **Praxishinweis:** Spezifisch zur **Minimierung** der Verarbeitung der Nutzerdaten in Gestalt sowohl der Anmeldedaten als auch der nutzerbezogenen Betriebsmitteldaten kann dabei der Einsatz von **Schnittstellen** (oftmals von Drittanbietern) beitragen, die gegebenenfalls eine **anonyme Nutzung** des betreffenden KI-Systems ermöglichen.

¹⁶⁵ Zum Ganzen DSK, Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode (Fn. 160).

ee) Weiterverarbeitung der eingegebenen Daten zum Training eines KI-Systems

Schließlich können die eingegebenen Daten je nach Konfiguration des KI-Systems zu dessen Weitertraining (weiter)verarbeitet werden. 185

Hinweise: Die Verarbeitung von Ein- und Ausgaben zum weiteren Training eines KI-Systems bedarf als zweckändernde Weiterverarbeitung dieser Daten einer eigenen Rechtsgrundlage sowie einer Zweckänderungsbefugnis. Gegebenenfalls ist eine Anonymisierung dieser Daten, beispielsweise durch Datenreduktion beziehungsweise -aggregation, zu prüfen. Eine solche anonymisierende Verarbeitung unterliegt allerdings denselben Rechtmäßigkeitsanforderungen. 186

Bei der Nutzung von KI-Systemen Dritter wird empfohlen, das Training mit den Eingabedaten durch entsprechende Konfiguration auszuschließen.

e) Nutzung von Ergebnissen der Künstlichen Intelligenz

Je nach Arbeitsauftrag und den im KI-System vorhandenen Daten enthält auch die **Ausgabe**, das heißt der Verarbeitungsvorgang „**Bereitstellung des Ergebnisses**“, personenbezogene Daten. 187

Dies kann aus einem **Aufgreifen von personenbezogenen Inhalten einer Arbeitsanweisung**, aus einer bloßen **Wiedergabe personenbezogener Trainingsdaten**, an die sich das System „erinnert“, oder aus einer **Neuverknüpfung von Daten** zur Ergebniserstellung, mit der die Herstellung eines Personenbezugs einhergeht, resultieren.¹⁶⁶ 188

Beispiel: Eine Beschäftigte einer Gemeinde lässt durch ein Großes Sprachmodell ein Grußwort für ein Vereinsjubiläum erstellen. Da das System unter anderem mit im Internet frei abrufbaren Daten trainiert wurde, die auch Namen von Vereinsmitgliedern umfassen, werden einige dieser Namen im auf die Anfrage erstellten Grußwort genannt.

Will die Beschäftigte der Gemeinde den von dem KI-System vorgeschlagenen Entwurf verwenden, muss sie insbesondere prüfen, ob die enthaltenen Daten richtig sind und ob eine Rechtsgrundlage für die Verarbeitung der Namen als personenbezogene Daten besteht.

Im Einzelfall kann ein Personenbezug auch erst **durch den Nutzer** eines KI-Systems hergestellt werden. 189

Beispiel: Ein von einem KI-System entworfenes neutrales Schreiben wird vom Sachbearbeiter an einen bestimmten Bürger adressiert.

Die öffentliche Stelle muss die Ausgaben eines KI-Systems vor einer Weiterverwendung mit hin auf einen etwaigen **Personenbezug sowie das Vorliegen einer Rechtsgrundlage für die entsprechende Datenverarbeitung prüfen**. Zudem darf sie die Ausgaben eines KI-Systems nicht „einfach so“ verwenden, sondern muss diese sorgfältig insbesondere hinsichtlich 190

¹⁶⁶ Ausführlich Pesch/Böhme, Verarbeitung personenbezogener Daten und Datenrichtigkeit bei großen Sprachmodellen, ChatGPT & Co. unter der DS-GVO, MMR 2023, S. 917, 921.

V. Datenschutz-Grundverordnung

ihrer **Diskriminierungsfreiheit, Richtigkeit und Vollständigkeit** bewerten (vgl. Art. 5 Abs. 1 Buchst. a, Buchst. d und Buchst. f DSGVO).¹⁶⁷

f) Bereiche oder Phasen von KI-Systemen ohne personenbezogene Daten

- 191 Gegebenenfalls gibt es abgrenzbare Bereiche oder Verarbeitungsphasen von KI-Systemen, in denen keinerlei personenbezogene Daten vorkommen, weder als Trainings-, Eingabe- oder Ausgabedaten noch im Anmelde- oder Verarbeitungsprozess. Solche Einsatzfelder unterliegen zwar nicht dem Datenschutzrecht, jedoch der KI-Verordnung.

3. Datenschutzrechtliche Anforderungen im Einzelnen

- 192 Verarbeitet ein KI-System personenbezogene Daten in dem beschriebenen Sinne, sind **sämtliche Anforderungen der Datenschutz-Grundverordnung**, insbesondere die Verarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO, das zwingende Erfordernis einer Rechtsgrundlage für die Datenverarbeitung gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO sowie die Informationspflichten nach Art. 12 ff. DSGVO und die Betroffenenrechte nach Art. 15 ff. DSGVO, zu beachten; der datenschutzrechtlich Verantwortliche muss die Einhaltung seiner Pflichten jederzeit nachweisen können, Art. 5 Abs. 2 DSGVO („**Rechenschaftspflicht**“).

a) Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO)

- 193 Art. 5 Abs. 1 DSGVO legt die Grundsätze für die Verarbeitung personenbezogener Daten fest.

aa) Rechtmäßigkeit, Treu und Glauben, Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO)

- 194 Art. 5 Abs. 1 Buchst. a DSGVO statuiert die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben sowie der Transparenz.
- 195 Der **Grundsatz der Rechtmäßigkeit**, der eine **Verarbeitung auf rechtmäßige Weise** fordert, wird durch **Art. 6 DSGVO** (bei Verarbeitungen besonderer Kategorien personenbezogener Daten in Verbindung mit Art. 9 DSGVO) dahingehend konkretisiert, dass eine Verarbeitung nur rechtmäßig ist, wenn mindestens eine der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen vorliegt (siehe Rn. 216 ff.).
- 196 Der **Grundsatz der Verarbeitung nach Treu und Glauben** erfordert allgemein formuliert eine „**faire**“ **Verarbeitung** (siehe „fairness“ in der englischen Sprachfassung der Datenschutz-Grundverordnung), wobei unter „unfairen“ Datenverarbeitungen beispielsweise verborgene, unerwartete oder übermäßige (das heißt nicht datensparsame) Verarbeitungen subsumiert werden. Insoweit kann sich insbesondere ein Konflikt mit diskriminierenden

¹⁶⁷ Zu möglichen Problemstellungen in diesem Zusammenhang siehe Rn. 135, 193 ff.

3. Datenschutzrechtliche Anforderungen

Ausgaben eines KI-Systems ergeben, die den Rückschluss auf eine unfaire Verarbeitung zulassen.¹⁶⁸

Beim **Grundsatz der Transparenz** geht es schließlich um die **Nachvollziehbarkeit der Verarbeitung für die betroffenen Personen** (vgl. **EG 39 Sätze 2 bis 5 DSGVO**). Die aus dem Transparenzgebot folgenden Pflichten sind insbesondere durch die Informationspflichten in **Art. 12 ff. DSGVO näher ausgestaltet**. In Bezug auf **Künstliche Intelligenz** erfordert die Herstellung von Transparenz – wie bei jeder Verarbeitung personenbezogener Daten – eine nachvollziehbare Information über die Verarbeitungsvorgänge (Art. 5 Abs. 1 Buchst. a DSGVO); steht eine automatisierte Entscheidungsfindung mittels Künstlicher Intelligenz im Raum, sind nach Art. 13 Abs. 2 Buchst. f, Art. 14 Abs. 2 Buchst. g DSGVO zusätzlich „aussagekräftige Informationen“ über die involvierte Logik¹⁶⁹ einschließlich der Tragweite und möglichen Auswirkungen für die betroffene Person zu geben.¹⁷⁰ Art. 12 Satz 1, EG 39 Satz 3, EG 58 DSGVO sehen ergänzend eine verständliche Darstellung in klarer und einfacher Sprache vor. Weitergehende Anforderungen, insbesondere an den Detaillierungsgrad dieser Informationen, enthält die Datenschutz-Grundverordnung dagegen nicht. Im Ergebnis können Informationen daher als hinreichend transparent in diesem Sinne angesehen werden, wenn sie der betroffenen Person allgemein – somit für jedermann verständlich – die sie betreffenden Verarbeitungsvorgänge darstellen. Da es sich bei Datenverarbeitungen im Zusammenhang mit der Nutzung von Künstlicher Intelligenz in der Regel um äußerst komplexe, auch für Entwickler nicht immer ganz nachvollziehbare Prozesse handelt, sollte es ausreichen, die Informationen auf die abstrakte Funktions- und Verfahrensweise des betreffenden KI-Systems zu beschränken, beispielsweise, indem die einzelnen Verarbeitungsschritte eines KI-Systems **von Anfang an soweit wie möglich nachvollzogen und für die einzelnen Nutzer ebenso schrittweise dargestellt** werden. Auch eine Unterstützung durch **Grafiken** bietet sich an.¹⁷¹

197

bb) Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO)

Der Grundsatz der Zweckbindung nach Art. 5 Abs. 1 Buchst. b DSGVO fordert eine **Datenerhebung für festgelegte, eindeutige und legitime Zwecke** und **untersagt eine Weiterverarbeitung der betreffenden personenbezogenen Daten in einer mit diesen Zwecken nicht zu vereinbarenden Weise**, mit eng gefassten Ausnahmen unter Berücksichtigung des Art. 89 Abs. 1 DSGVO für Weiterverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

198

Hinweis: Diese Privilegierungen finden für Entwicklung, Training und Nutzung rein kommerzieller KI-Systeme keine Anwendung.

199

¹⁶⁸ Siehe DSK, Hambacher Erklärung (Fn. 107), S. 3 f.

¹⁶⁹ EuGH, Urteil vom 27. Februar 2025, C-203/22, vgl. Rn. 338. Siehe auch DSK, Hambacher Erklärung (Fn. 107), S. 3.

¹⁷⁰ DSK, Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024, Künstliche Intelligenz und Datenschutz, Orientierungshilfe, Rn. 22, Internet: https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

¹⁷¹ Zu den Informationspflichten ausführlich siehe Rn. 296 ff.

V. Datenschutz-Grundverordnung

- 200 Diese Anforderungen mögen sich auf den ersten Blick nicht mit der Künstlichen Intelligenz immanenten **Autonomie, Anpassungs- und Lernfähigkeit** (vgl. Art. 3 Nr. 1 KI-Verordnung) vertragen.¹⁷²
- 201 Für die Anwendung des Zweckbindungsgrundsatzes auf KI-Systeme gilt dabei grundsätzlich: Wird ein KI-System für einen bestimmten Zweck entwickelt, ist anzunehmen, dass der **Zweck in der Entwicklungsphase in direktem Zusammenhang mit dem mit der Verarbeitung in der Einsatzphase verfolgten Zweck** steht – unabhängig von der jeweiligen datenschutzrechtlichen Verantwortlichkeit. Diese Zweckbestimmung kann im Einzelfall – eine entsprechende Klarstellung und Erforderlichkeit vorausgesetzt – auch die Verarbeitung personenbezogener Daten zur Vermeidung von (potenziellen) Verzerrungen oder Fehlern umfassen.¹⁷³
- 202 Werden KI-Systeme **ohne einen konkreten Einsatzzweck** entwickelt, kann es schwierig sein, einen expliziten, ausreichend spezifizierten Zweck der Datenverarbeitung in der Entwicklungsphase festzulegen. Dies ist beispielsweise bei KI-Systemen mit allgemeinem Verwendungszweck der Fall, die für eine Vielzahl von Zwecken eingesetzt werden können. Unter Berücksichtigung der Besonderheiten von KI-Systemen dürfte jedenfalls dann eine festgelegte, eindeutige und legitime Zwecksetzung im Sinne des Art. 5 Abs. 1 Buchst. b DSGVO vorliegen, wenn die „**Art“ des entwickelten, zugrundeliegenden KI-Modells**, dessen **erwartete Funktionalitäten sowie andere relevante, zu diesem Zeitpunkt bereits bekannte Informationen** hinreichend **klar, verständlich und spezifisch** dargestellt werden.¹⁷⁴ Gegebenenfalls kann eine (weitere) Zweckkonkretisierung durch den Verantwortlichen auch noch im Laufe des Prozesses erfolgen.¹⁷⁵
- 203 Deutlich werden die mit dem Erfordernis der Zweckbindung verbundenen Herausforderungen beispielsweise auch im Zusammenhang mit Großen Sprachmodellen, welche häufig von Nutzern eingegebene Daten nicht nur zur „Beantwortung“ eines konkreten Prompts, sondern auch zum **Weitertraining** des Systems verwenden. Gegebenenfalls ist zu prüfen, inwieweit die Anforderungen an eine **Zweckänderung** erfüllt sind (siehe Art. 6 Abs. 4 DSGVO und Art. 6 BayDSG, Rn. 268 ff.).¹⁷⁶ Die gesetzlichen Regelungen sehen insoweit nur wenige eng begrenzte Ausnahmen vom Grundsatz der Zweckbindung vor.
- 204 **Hinweis:** Eine explizite Ausnahme findet sich beispielsweise in der **Verordnung über den europäischen Gesundheitsdatenraum**:¹⁷⁷ diese nennt in **Art. 53 Abs. 1 Buchst. e Ziff. ii** das **KI-Training** ausdrücklich als einen **Zweck, zu dem elektronische Gesundheitsdaten zur Sekundärnutzung** verarbeitet werden können.

¹⁷² Vergleiche m. w. N. Paal, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, ZfDR 2024, S. 129, 143.

¹⁷³ EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 64.

¹⁷⁴ EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 64.

¹⁷⁵ Vergleiche Paal, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, ZfDR 2024, S. 129, 144.

¹⁷⁶ Vergleiche DSK, Hambacher Erklärung (Fn. 107), S. 3.

¹⁷⁷ Fn. 102.

3. Datenschutzrechtliche Anforderungen

Für bayerische öffentliche Stellen folgt daher aus dem Zweckbindungsgrundsatz das Erfordernis der Festlegung konkreter Zwecke im Rahmen ihrer Aufgabenerfüllung, für welche Künstliche Intelligenz eingesetzt werden darf, beziehungsweise für welche Zwecke mittels Künstlicher Intelligenz personenbezogene Daten verarbeitet werden dürfen. Dies umfasst auch die Prüfung etwaiger Drittprodukte dahingehend, ob beispielsweise ein Weitertraining deaktiviert werden kann, sofern hierfür keine Rechtsgrundlage vorliegt. 205

cc) Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO)

Das Training von KI-Systemen bedarf grundsätzlich vieler – regelmäßig auch personenbezogener – Echtdaten. Demgegenüber regelt Art. 5 Abs. 1 Buchst. c DSGVO den Grundsatz der Datenminimierung, der besagt, dass personenbezogene **Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt** sein müssen. 206

Zur Umsetzung des Grundsatzes der Datenminimierung im Zusammenhang mit der Nutzung von KI-Systemen sind neben der Beschränkung der personenbezogenen (Trainings-)Daten auf das notwendige **Maß** die ausschließliche Nutzung von **anonymisierten** Daten oder zumindest von Maßnahmen des „**Privacy Enhancing**“ in Erwägung zu ziehen.¹⁷⁸ Weitere denkbare Maßnahmen zur Datenminimierung sind beispielsweise **vorgeschaltete Prompt- und/oder Output-Filter oder vergleichbare Technologien** zur Einschränkung beziehungsweise Standardisierung des In- und/oder Outputs, um die Ein- und/oder Ausgabe personenbezogener Daten so weit wie möglich zu verhindern, oder **Datendepublikation**, das heißt die Identifizierung und Entfernung doppelter Datensätze. Zudem sollten Nutzer mittels **Schulungen und Informationsmaterial** dabei unterstützt werden, ihre Eingaben bei Nutzung von KI-Systemen möglichst datensparsam zu gestalten. Gleichzeitig ist stets der für die Gewährleistung der Qualität eines KI-Modells **konkret erforderliche Datenumfang** zu berücksichtigen – nach der KI-Verordnung müssen KI-Systeme fair, hinreichend präzise und sicher sein und dürfen nicht unzulässig diskriminieren; zur Erfüllung dieser Pflichten kann es im Einzelfall umfangreicher Datensätze bedürfen. 207

dd) Richtigkeit (Art. 5 Abs. 1 Buchst. d DSGVO)

Großen Sprachmodellen wird immer wieder **eine Neigung zum „Halluzinieren“ zugeschrieben**, das heißt zum Generieren falscher oder irreführender Ergebnisse, beispielsweise aufgrund von unzureichenden oder Bias-behafteten Trainingsdaten oder falschen Annahmen des KI-Modells.¹⁷⁹ In diesem Zusammenhang kommt aus Datenschutzsicht dem Grundsatz der Richtigkeit nach Art. 5 Abs. 1 Buchst. d DSGVO besondere Bedeutung zu.¹⁸⁰ Dieser 208

¹⁷⁸ Siehe DSK, Hambacher Erklärung (Fn. 107), S. 4; Paal, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, ZfDR 2024, S. 129, 141 f.

¹⁷⁹ Siehe BSI, Generative KI-Modelle - Chancen und Risiken für Industrie und Behörden, Version 1.1 vom 27. März 2024, S. 9, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.html.

¹⁸⁰ Ausführlich zum Datenrichtigkeitsgebot bei LLM siehe Pesch/Böhme, Verarbeitung personenbezogener Daten und Datenrichtigkeit bei großen Sprachmodellen, ChatGPT & Co. unter der DS-GVO, MMR 2023, S. 917, 921 f.

V. Datenschutz-Grundverordnung

Grundsatz erfordert, dass **personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand** sein müssen und **alle angemessenen Maßnahmen** zu treffen sind, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. In der Praxis ist daher aufgrund der Möglichkeit der Ausgabe von halluzinierten Informationen durch ein KI-System der **Inhalt einer Ausgabe vor der Verwendung stets umfassend zu überprüfen**.

Beispiel: Ein Gemeindebediensteter, der von einem Großen Sprachmodell ein Grußwort für ein Jubiläum erstellen lässt, kommt also um eine Qualitätssicherung nicht herum. Er muss dafür sorgen, dass dem Jubilar keine personenbezogenen Daten zugeschrieben werden, die nicht stimmen. Geschieht dies nicht, kann der Jubilar von der Gemeinde Berichtigung, je nach Lage des Falls auch Schadenersatz verlangen.

- 209 Ein weiteres Risiko für die Datenrichtigkeit besteht im Hinblick auf den **Aktualitätsstand** der Trainingsdaten: So werden beispielsweise KI-Systeme lediglich bis zu einem bestimmten Zeitpunkt trainiert und dann – ohne Echtzeit-Anschluss an das Internet oder Datenbanken – auf den Markt gebracht.
- 210 Betroffene Personen haben bei der Verarbeitung unrichtiger personenbezogener Daten das Recht auf Berichtigung nach **Art. 16 DSGVO** sowie das Recht auf Löschung nach **Art. 17 DSGVO**.¹⁸¹

ee) Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO)

- 211 Der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 Buchst. e Halbsatz 1 DSGVO besagt in Ergänzung des Grundsatzes der Zweckbindung nach Art. 5 Abs. 1 Buchst. b DSGVO in zeitlicher Hinsicht, dass personenbezogene Daten **in einer Form gespeichert** werden müssen, welche die **Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich** ist. Die Speicherbegrenzung ist damit auf die Bestimmbarkeit von personenbezogenen Daten bezogen. **Ausnahme** dürfen personenbezogene Daten gemäß Art. 5 Abs. 1 Buchst. e Halbsatz 2 DSGVO länger gespeichert werden, soweit diese vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von der Datenschutz-Grundverordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß **Art. 89 Abs. 1 DSGVO** verarbeitet werden. Klarstellend fordert **EG 39 Satz 8 DSGVO**, dass die Speicherfrist für personenbezogene Daten auf das **unbedingt erforderliche Mindestmaß** beschränkt bleibt.
- 212 Der Grundsatz der Speicherbegrenzung gilt für alle Formen der Datenverarbeitung¹⁸² und wird unter anderem durch das Recht der betroffenen Personen auf Löschung (**Art. 17 DSGVO**) ausgestaltet (hierzu Rn. 322 ff.).

¹⁸¹ Siehe unten Rn. 322 ff.

¹⁸² Roßnagel, in Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2. Aufl. 2025, Art. 5 DSGVO Rn. 152.

3. Datenschutzrechtliche Anforderungen

In Zusammenhang mit KI-Systemen und der damit verbundenen grundsätzlich dauerhaften Speicherung zumindest der Trainingsdaten bedarf es insoweit einer entsprechenden (datenschutzrechtlichen) Begründung. Zu berücksichtigen ist dabei, dass die Zweckfestsetzung des Verantwortlichen nach Art. 5 Abs. 1 Buchst. b DSGVO den maßgeblichen Orientierungspunkt des Grundsatzes der Speicherbegrenzung darstellt und der Verantwortliche prüfen muss, ob er für den von ihm festgelegten Zweck den Personenbezug (noch) benötigt im Sinne einer Zweck-Mittel-Relation. Der Verantwortliche könnte insoweit – unter Vorlage entsprechender Nachweise, möglicherweise auf Grundlage der Algorithmen – zum Beispiel die Erforderlichkeit der Daten für die (qualitativ hochwertige) Funktion eines KI-Systems als Begründung vorbringen. 213

ff) Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO)

Der Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO) fordert, dass personenbezogene Daten **in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten gewährleistet**. Er wird **durch Art. 32 DSGVO ausgestaltet** und verlangt, dass geeignete technische und organisatorische Maßnahmen getroffen werden, die insbesondere dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung dienen (näher Rn. 343 ff.). 214

Beim Einsatz von KI-Systemen betrifft dies beispielsweise die **Abwehr von „Privacy Attacks“**, mit welchen unter Umständen Informationen über Trainings- und Inhaltsdaten rekonstruiert beziehungsweise extrahiert werden können oder auf Eingaben zugegriffen werden kann.¹⁸³ Derartige Schwachstellen und Missbrauchsmöglichkeiten müssen grundsätzlich bereits vor Produktivsetzung eines KI-Systems, beispielsweise mittels **„Red-Teaming“**, ermittelt¹⁸⁴ und auf der Grundlage der gewonnenen Erkenntnisse dann korrespondierende Schutzmaßnahmen etabliert werden. Aber auch während der Nutzung eines KI-Systems muss der Verantwortliche dessen Sicherheit gewährleisten und in regelmäßigen Abständen entsprechende Risikoabwägungen und Überprüfungen vornehmen, gerade auch unter Berücksichtigung technischer Entwicklungen. 215

b) Rechtsgrundlagen

Dem **Grundsatz der Rechtmäßigkeit** nach Art. 5 Abs. 1 Buchst. a DSGVO entsprechend ist eine Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn sie auf mindestens eine der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen gestützt werden kann (siehe oben Rn. 216 ff.)¹⁸⁵ und bei Daten nach Art. 9 Abs. 1 DSGVO die zusätzlichen Anforderungen 216

¹⁸³ Siehe hierzu und zu weiteren Angriffen auf KI-Anwendungen m. w. N. BSI, Generative KI-Modelle – Chancen und Risiken für Industrie und Behörden (Fn. 179), S. 14 ff.

¹⁸⁴ International Working Group on Data Protection in Technology, Working Paper on Large Language Models (LLMs) (Fn. 143), S. 11.

¹⁸⁵ Die Datenschutz-Grundverordnung sieht kein Hierarchieverhältnis der verschiedenen Rechtsgrundlagen untereinander vor, vgl. EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Stand 10/2024, Rn. 1, Internet: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.

V. Datenschutz-Grundverordnung

aus Art. 9 Abs. 2 DSGVO gewahrt sind.¹⁸⁶ Dabei ist **jeder einzelne Verarbeitungsvorgang separat** zu betrachten – auch bei der Verarbeitung personenbezogener Daten durch KI-Systeme (zu einzelnen Vorgängen siehe Rn. 138 ff.).

- 217 Insoweit gilt ganz grundsätzlich: **Öffentliche Stellen** dürfen personenbezogene Daten **in der Regel** verarbeiten, wenn die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (**Art. 6 Abs. 1 UAbs. 1 Buchst. c**, Abs. 3 DSGVO in Verbindung mit einer Verpflichtung nach unioalem oder nationalem Recht) oder zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (**Art. 6 Abs. 1 UAbs. 1 Buchst. e**, Abs. 3 DSGVO in Verbindung mit einer unionsrechtlichen oder nationalrechtlichen Verarbeitungsbefugnis). Auf die Rechtsgrundlage des „berechtigten Interesses“ nach **Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO**¹⁸⁷ können sich **Behörden** dagegen für die **in Erfüllung ihrer Aufgaben** vorgenommenen Verarbeitungen **nicht** berufen, Art. 6 Abs. 1 UAbs. 2 DSGVO.
- 218 KI-Systeme können in diesem Rahmen als **Betriebsmittel** zum Einsatz kommen. Dabei ist im Einzelfall sorgfältig zu prüfen, welche Auswirkungen die Nutzung der KI-Systeme zur Verarbeitung personenbezogener Daten aufgrund ihrer spezifischen Besonderheiten auf die Grundrechte und Grundfreiheiten der betroffenen Personen hat und **ob die jeweilige Rechtsgrundlage für die Verarbeitung deren Einsatz rechtfertigt oder aufgrund der besonderen Schwere des Grundrechtseingriffs (der Erlass) eine(r) spezialgesetzliche(n) Regelung** für Datenverarbeitungen mittels Künstliche Intelligenz erforderlich ist (unter Beachtung der Vorgaben insbesondere des Art. 6 Abs. 2 und 3 DSGVO). Gerade im Bereich der Sicherheit und bei Kernfragen des persönlichen Lebensbereichs wird die allgemeine Aufgaben- oder Befugnisnorm in vielen Fällen nicht ausreichen, sondern eine explizite Rechtsgrundlage erforderlich sein, die der Schwere des Grundrechtseingriffs gerecht wird.
- 219 Im Folgenden werden die einzelnen Rechtsgrundlagen im Sinne von Art. 6 Abs. 1 und Art. 9 Abs. 2 DSGVO dargestellt, die für Verarbeitungen personenbezogener Daten mittels Künstlicher Intelligenz durch bayerische öffentliche Stellen von besonderem Interesse sind:

¹⁸⁶ EuGH, Urteil vom 21. Dezember 2023, C-667/21.

¹⁸⁷ Nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Vergleiche hierzu EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Fn. 185). Als Abwägungskriterien sind dabei im Zusammenhang mit KI-Anwendungen insbesondere die (Un-)Kenntnis der betroffenen Personen, datensicherheitsspezifische Verarbeitungsrisiken, die Verarbeitung sensibler Daten, aber auch gezielte technische Schutzmaßnahmen wie eine umfassende und effektive Anonymisierung oder Pseudonymisierung, hohe Transparenz-Standards oder der Einsatz von Filtersystemen zu berücksichtigen. Hierzu auch EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 66 ff. sowie zu risikomindernden Maßnahmen Rn. 96 ff. Für eine Prägung der vernünftigen Erwartungen des Einzelnen durch einschlägige Vorgaben des Unionsrechts, wie die KI-Verordnung, Fuchs/Wünschelbaum/Hansen/Walczak, The Bridge Blueprint. Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim KI-Einsatz (Fn. 122), S. 3 f. Zu Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO als mögliche Rechtsgrundlage für Datenverarbeitungen zu KI-Trainingszwecken Oberlandesgericht Köln, Urteil vom 23. Mai 2025, 15 UKI 2/25.

aa) Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO)

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO rechtmäßig, wenn sie **zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist**, der der Verantwortliche unterliegt. Diese rechtliche Verpflichtung muss sich ausweislich **Art. 6 Abs. 3 DSGVO** aus **Unionsrecht oder nationalem Recht** ergeben. Die betreffende Datenverarbeitung muss mithin rechtlich angeordnet sein, wobei sich diese Verpflichtung auch aus einer **Präzisierung des mitgliedstaatlichen Rechts durch die Rechtsprechung** dieses Mitgliedstaats ergeben kann.¹⁸⁸ Dem Verantwortlichen kommt **keine Entscheidungsfreiheit** hinsichtlich der Erfüllung der rechtlichen Pflicht zu; zudem sind Verarbeitungen in diesem Rahmen auf das für die Erreichung des Verarbeitungszwecks (hierzu Art. 6 Abs. 3 Buchst. b Satz 2 DSGVO) **absolut Notwendige**¹⁸⁹ zu beschränken. 220

Aufgrund dieser Vorgaben hat die Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO in Bezug auf die Verarbeitung personenbezogener Daten durch **KI-Systeme** mit Blick auf deren regelmäßige Vielzahl an Rechenleistungen **bisher allenfalls untergeordnete Bedeutung**. Insbesondere ist derzeit keine gesetzlich normierte **Verpflichtung** für (Weiter-) Training oder Nutzung von KI-Systemen bekannt. 221

bb) Aufgabenwahrnehmung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO)

Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO gestattet die Verarbeitung personenbezogener Daten durch öffentliche Stellen, sofern diese **für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt**, die dem Verantwortlichen übertragen wurde. 222

Beide Varianten setzen dabei nach **Art. 6 Abs. 3 DSGVO** die Übertragung einer entsprechenden Aufgabe an den Verantwortlichen durch **Unionsrecht oder nationales Recht** sowie eine Verarbeitungsbefugnis voraus. Diese kann sich insbesondere aus nationalem **Fachrecht** ergeben (zum Beispiel für Personalaktendaten nach dem Bayerischen Beamtenengesetz oder für Sozialdaten nach dem Zehnten Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz [SGB X]). Die Erforderlichkeit und Verhältnismäßigkeit der Datenverarbeitung mittels des Betriebsmittels „Künstliche Intelligenz“ für die Aufgabenerfüllung ist dabei jeweils im Einzelfall darzulegen und zu begründen (hierzu gleich Rn. 227 ff.). 223

¹⁸⁸ EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22. Voraussetzung ist, dass diese Rechtsprechung klar und präzise ist, ihre Anwendung für die Rechtsunterworfenen vorhersehbar ist und sie ein im öffentlichen Interesse liegendes Ziel verfolgt, zu dem sie in einem angemessenen Verhältnis steht.

¹⁸⁹ Vergleiche im Einzelnen Buchner/Petri, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 6 DSGVO Rn. 81, 82.

V. Datenschutz-Grundverordnung

- 224 Nachrangig hierzu stehen die **Auffangnormen des Art. 4 und Art. 5 BayDSG**, die nur dann zur Anwendung kommen, sofern nicht spezifischere Vorschriften die Verarbeitung insoweit abschließend regeln.
- 225 Mit Blick auf den Bestimmtheits- und Verhältnismäßigkeitsgrundsatz kommen die vorgenannten allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes jedoch nur für Datenverarbeitungen mit **geringer Eingriffsintensität**¹⁹⁰ und auch **nicht für massenhafte Datenverarbeitungen** in Betracht. Beim Einsatz von KI-Systemen könnte schon deren (oftmals) nicht vollständige Erklärbarkeit für einen schwerwiegenden Eingriff sprechen und damit den Rückgriff auf Art. 4 und 5 BayDSG ausschließen; hinzu kommt die mit dem Einsatz von Künstlicher Intelligenz regelmäßig verbundene unbeschränkte Anzahl an Datenverarbeitungen.
- 226 Zudem erlaubt die Generalklausel des **Art. 4 Abs. 1 BayDSG Datenverarbeitungen durch öffentliche Stellen nur, wenn und soweit sie zur (rechtmäßigen) Erfüllung der ihnen obliegenden Aufgaben erforderlich** sind. Es bedarf mithin einer entsprechenden Aufgabenzuweisung; die Datenverarbeitung muss ferner zur Erfüllung dieser Aufgabe **erforderlich** sein.
- 227 EG 39 Satz 7 DSGVO liefert Hinweise, was unter dem **Erforderlichkeitskriterium** zu verstehen ist: Danach sollten personenbezogene Daten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Zudem dürfen sie nur verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (EG 39 Satz 10 DSGVO). Die **bloße Sachdienlichkeit oder Förderlichkeit** der Datenverarbeitung zur Erfüllung einer konkreten Aufgabe genügt hierfür **nicht**. Dies bedeutet speziell mit Blick auf die Nutzung von Künstlicher Intelligenz, dass es **kein anderes gleich geeignetes milderes Mittel als die Datenverarbeitung mittels KI-Systemen** geben darf; so begründen eine rein beschleunigende Wirkung von KI-Systemen auf Prozesse oder eine kostengünstigere Datenverarbeitung alleine noch keine Erforderlichkeit in diesem Sinne.
- 228 **Hinweise:** Insbesondere das initiale Training eines KI-Systems wird daher in der Regel nicht als im strengen Sinne erforderlich für die Erfüllung einer konkreten Aufgabe anzusehen sein. Insoweit bedarf es für bayerische öffentliche Stellen nationalrechtlicher (fach-)gesetzlicher Verarbeitungsbefugnisse, die das Training mit personenbezogenen Daten und gegebenenfalls deren Weiterverarbeitung in KI-Systemen regeln. Derzeit gibt es in Bayern noch keine solchen Regelungen.¹⁹¹ Die zu schaffenden (fach-)gesetzlichen Verarbeitungsbefugnisse im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO müssen inhaltlich den Anforderungen des Art. 6 Abs. 2 und 3 DSGVO entsprechen. Zudem müssten sie im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten die Ausnahmen nach Art. 9 Abs. 2 DSGVO begründen (s. hierzu Rn. 253 ff.). Wäre mit der Datenverarbeitung – wie beim Einsatz von KI-

¹⁹⁰ So zuletzt Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267.

¹⁹¹ Die Notwendigkeit derartiger Verarbeitungsbefugnisse erkannte die Bayerische Staatsregierung allerdings bereits in ihrem Digitalplan Bayern. Dort (Stand 3/2023, S. 70, Internet: <https://digitalplan.bayern/bayern/de/home>) ist ausdrücklich die Schaffung von rechtlichen Grundlagen dafür, die Daten den zuständigen Einheiten der öffentlichen Hand zur Verarbeitung mittels modernster Datenverarbeitungsmethoden zuzuführen, vorgesehen.

3. Datenschutzrechtliche Anforderungen

Systemen häufig – eine automatisierte Entscheidung im Einzelfall im Sinne von Art. 22 DSGVO verbunden, sind zugleich dessen Vorgaben einzuhalten (siehe im Einzelnen Rn. 329 ff.).

Art. 5 BayDSG statuiert mit entsprechenden Vorgaben **spezifische Regelungen für Übermittlungen** von personenbezogenen Daten. 229

cc) Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO)

Nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn die betroffene Person ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.¹⁹² Eine wirksame Einwilligung in diesem Sinne setzt dabei nach **Art. 4 Nr. 11 DSGVO** insbesondere eine freiwillige, unmissverständlich abgegebene und hinreichend bestimmte Willensbekundung in informierter Weise voraus. **Art. 7 DSGVO** konkretisiert die Bedingungen für die Abgabe der Einwilligung näher. 230

Im Kontext von Datenverarbeitungen mittels **Künstlicher Intelligenz** durch **öffentliche Stellen** ergibt sich im Hinblick auf die einzelnen Tatbestandsvoraussetzungen der Einwilligung eine Vielzahl von **Besonderheiten**: 231

So kommt der Rechtsgrundlage der Einwilligung im **Verhältnis zwischen Bürger und Staat** schon grundsätzlich **nur eingeschränkte Relevanz** zu, da das **Kriterium der Freiwilligkeit in dieser Konstellation kritisch** zu sehen ist: Notwendig für die Freiwilligkeit ist ein freier Willensentschluss, das heißt eine echte und freie Wahl (**EG 42 DSGVO**). Nach EG 43 Satz 1 DSGVO soll eine Einwilligung keine taugliche Rechtsgrundlage darstellen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt und es deshalb in Betracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde.¹⁹³ 232

Hinweis: Ein vergleichbares Ungleichgewicht wird auch aufgrund von Abhängigkeiten im Beschäftigungsverhältnis zwischen Arbeitgebern und Beschäftigten sowie Dienstherrn und Beamten in der Regel vorliegen. 233

Die Freiwilligkeit im Sinne einer echten und freien Wahl kann im Zusammenhang mit dem Einsatz von KI-Systemen im Einzelfall zudem wegen Einflüssen durch beispielsweise **Lock-** 234

¹⁹² Ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 9/2021, Internet: <https://www.datenschutz-bayern.de/infothek/>.

¹⁹³ Ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung (Fn. 192), Rn 71.

V. Datenschutz-Grundverordnung

in-Effekte¹⁹⁴, **Nudging**¹⁹⁵ und **Dark Patterns** beziehungsweise **Deceptive Design Patterns**¹⁹⁶ in Frage stehen.

- 235 Schließlich gilt gemäß **EG 43 Satz 2 DSGVO** eine Einwilligung auch dann nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist (Erfordernis der sogenannten **Granularität** der Einwilligung), oder wenn die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von einer Einwilligung abhängig gemacht wird, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist (sogenanntes **Koppelungsverbot, Art. 7 Abs. 4 DSGVO**).
- 236 Damit eine Einwilligung **hinreichend bestimmt** ist, muss der Verantwortliche vorab unter anderem festlegen, welche Daten für welche Zwecke auf welche Weise von wem verarbeitet werden und wer die Empfänger dieser Daten sind, um der betroffenen Person die Möglichkeit zu geben zu überprüfen, ob sie eine Einwilligung zu der ihre personenbezogenen Daten betreffenden Verarbeitung erteilen möchte. Die konkreten Anforderungen an die Bestimmtheit sind im Einzelfall unter Berücksichtigung der jeweiligen Eingriffsintensität der Datenverarbeitung festzustellen. Eine Einwilligung als Rechtsgrundlage setzt mithin voraus, dass die Struktur und die Rahmenbedingungen der betreffenden Datenverarbeitung hinreichend bestimmt sind.
- 237 **Hinweis:** Im Zusammenhang mit den Verarbeitungsvorgängen „Sammeln personenbezogener Daten für ein KI-System“ sowie „Training eines KI-Systems mit personenbezogenen Daten“ stehen die spätere konkret beabsichtigte Verarbeitung mit dem KI-System und deren Zweckbezug oftmals noch nicht abschließend fest, und eine Einwilligung kann nur in Bezug auf die genannten Verarbeitungsvorgänge, nicht aber in Bezug auf spätere Einsatzszenarien eingeholt werden.
- 238 Eng verbunden hiermit ist das Erfordernis einer **informierten Erklärung**, wonach der Verantwortliche die betroffene Person über die wesentlichen Aspekte der in Rede stehenden Datenverarbeitung zu informieren hat. Nach **EG 42 Satz 4 DSGVO** sind dies mindestens Informationen über den Verantwortlichen sowie die Zwecke der Datenverarbeitung, mit Blick auf die Rechtsprechung aber zusätzlich auch die Informationen nach **Art. 12 und 13 DSGVO**.¹⁹⁷

¹⁹⁴ Ein Lock-in-Effekt besteht dann, wenn aufgrund von technischen, prozessualen oder vertraglichen Abhängigkeiten eine freie Entscheidung nicht mehr möglich ist.

¹⁹⁵ Nudging beschreibt eine „sanfte Beeinflussung“ des Verhaltens oder auch der Entscheidungen, bei Besuchern von Websites beispielsweise durch bestimmte graphische Gestaltungen.

¹⁹⁶ Unter Dark Patterns beziehungsweise Deceptive Design Patterns versteht man manipulative Designs oder Prozesse, die Nutzer einer Website oder einer App zu einer Handlung „überreden“ sollen. Zu solchen „irreführenden Gestaltungsmustern“ vgl. auch EDSA, Leitlinien 03/2022 zu irreführenden Gestaltungsmustern auf Benutzeroberflächen von Social-Media-Plattformen: wie man sie erkennt und vermeidet, Version 2.0, 14. Februar 2023, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en. Zur Beeinflussung speziell durch KI-Systeme Sierke, Blinde Flecken im europäischen Verbraucher:innenleitbild – Dark Patterns und Dark AI, Max Planck Private Law Research Paper No. 26/2, Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6358805.

¹⁹⁷ EuGH, Urteil vom 11. Juli 2024, C-757/22, Rn. 60: „Die Gültigkeit der von der betroffenen Person erteilten Einwilligung hängt nämlich u. a. davon ab, ob diese Person zuvor die Informationen über alle Umstände im

3. Datenschutzrechtliche Anforderungen

Praxishinweis: Insbesondere die **Informationspflicht zu Verarbeitungszwecken** nach Art. 13 Abs. 1 Buchst. c DSGVO soll die betroffene Person in die Lage versetzen, **Anlass und Umfang der Verarbeitung ihrer personenbezogenen Daten zu überblicken**. Aus diesem Grund wird **empfohlen**, mit Blick auf die Risiken von Datenverarbeitungen mittels Künstlicher Intelligenz die betroffenen Personen **auch hinsichtlich der „Form der Verarbeitung“ und des hierfür eingesetzten Betriebsmittels „KI-System“** zu informieren, vergleiche EG 60 Satz 2 DSGVO. 239

Die Umsetzung dieser Anforderungen an Bestimmtheit und Informiertheit wird **durch die Intransparenz und oftmals mangelnde Nachvollziehbarkeit von komplexen KI-Systemen erschwert**. Hinzu kommt, dass die Informationen für die betroffenen Personen gemäß **Art. 12 Satz 1, EG 58 Satz 1 DSGVO** in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache abgefasst sein müssen. Zum Ganzen näher unten Rn. 296 ff. 240

Im Kontext der Einwilligung einschränkend zu beachten ist schließlich die **jederzeitige Widerruflichkeit nach Art. 7 Abs. 3 Satz 1 DSGVO**, von der die betroffene Person vor Abgabe ihrer Einwilligung in Kenntnis zu setzen ist, Art. 7 Abs. 3 Satz 3 DSGVO (vgl. auch Art. 13 Abs. 2 Buchst. c und Art. 14 Abs. 2 Buchst. d DSGVO). Macht die betroffene Person von ihrem Widerrufsrecht Gebrauch, so wird zwar die **Rechtmäßigkeit der bis zu diesem Zeitpunkt erfolgten Verarbeitung nicht berührt, Art. 7 Abs. 3 Satz 2 DSGVO**. Der Verantwortliche hat jedoch gemäß **Art. 17 Abs. 1 Buchst. b DSGVO**¹⁹⁸ ihre personenbezogenen **Daten unverzüglich zu löschen**, sofern keine anderweitige Rechtsgrundlage für deren Verarbeitung vorliegt und keiner der Ausnahmetatbestände des Art. 17 Abs. 3 DSGVO Anwendung findet. 241

Die **Umsetzung dieses Rechts auf Löschung** kann in KI-Systemen im Einzelfall technisch herausfordernd und nur mit unverhältnismäßigem Aufwand umsetzbar sein, da hierfür oftmals auf den Algorithmus des Systems eingewirkt werden muss. Je nach Konzeption können entsprechende Löschungen sich sogar auf die Funktionsfähigkeit des Systems insgesamt auswirken. Soll die Datenverarbeitung mittels Künstlicher Intelligenz auf Einwilligungen der betroffenen Personen gestützt werden, muss daher die Möglichkeit des Widerrufs nach Art. 7 Abs. 3 Satz 1 DSGVO von Anfang an mitgedacht werden, das heißt, es müssen **Prozesse etabliert und technische Gestaltungen vorgenommen** werden, die die gezielte Löschung von Daten ermöglichen, ohne die Funktionsfähigkeit des Systems vom Vorhandensein dieser Daten abhängig zu machen. 242

Für **Einwilligungen von Kindern in Bezug auf Dienste der Informationsgesellschaft** gelten die **besonderen Bedingungen des Art. 8 DSGVO** unter Beachtung der Grenzen der **Einwilligungsfähigkeit**. Werden **besondere Kategorien personenbezogener Daten** nach Art. 9 Abs. 1 DSGVO verarbeitet, kommt eine Einwilligung nach **Art. 9 Abs. 2 Buchst. a DSGVO** in Betracht (hierzu unten Rn. 260 f.). Schließlich ist eine Einwilligung auch für die **Übermittlung personenbezogener Daten an Drittländer** denkbar, **Art. 49 Abs. 1 Satz 1** 243

Zusammenhang mit der Verarbeitung der fraglichen Daten erhalten hat, auf die sie nach den Art. 12 und 13 DSGVO Anspruch hat und die ihr ermöglichen, die Einwilligung in voller Kenntnis der Sachlage abzugeben.“

¹⁹⁸ Zum Recht auf Löschung nach Art. 17 DSGVO allgemein siehe unten Rn. 322 ff.

V. Datenschutz-Grundverordnung

Buchst. a DSGVO (zu den gesetzlichen Vorgaben betreffend Drittlandübermittlungen allgemein siehe Rn. 358 ff.).

- 244 Insgesamt stößt die Einwilligung auch dort an ihre **Grenzen**, wo sie schon allein faktisch nicht eingeholt werden kann: Etwa bei einer Vielzahl von Trainingsdaten aus öffentlich zugänglichen Quellen, die personenbezogene Daten, aber keine realistisch umsetzbaren Kontaktmöglichkeiten enthalten. Wo ein Personenbezug erst durch Verschneidung oder das Vorliegen von Datenkategorien im Sinne von Art. 9 Abs. 1 DSGVO und Art. 10 DSGVO erst im Rahmen von verschiedenen Verarbeitungsvorgängen hergestellt wird, wird das Einholen einer Einwilligung ebenfalls regelmäßig nicht möglich sein.

dd) Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO)

- 245 Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO erlaubt die Verarbeitung personenbezogener Daten, soweit sie für **die Erfüllung eines Vertrags mit der betroffenen Person als Vertragspartei** (Variante 1) oder **zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person** (Variante 2) **erforderlich** ist. Derartige Vertragskonstellationen sind **auch unter Beteiligung öffentlicher Stellen denkbar**, beispielsweise im Zusammenhang mit der Durchführung öffentlich vergebener Aufträge oder – teilweise – bei der Erbringung von Leistungen der Daseinsvorsorge.
- 246 Voraussetzung für Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO ist zum einen ein **konkretes vertragliches oder vorvertragliches Verhältnis**, einschließlich der Vertragsbeendigung und -abwicklung,¹⁹⁹ **unter Einbindung der betroffenen Person**. Eine Verarbeitung personenbezogener **Daten Dritter**, die nicht Partei des Vertrags oder Anfragende vorvertraglicher Maßnahmen sind, kann daher **nicht** auf die Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO gestützt werden.²⁰⁰ **Ebenso wenig** sind (vorvertragliche) Maßnahmen zu Zwecken der **Preispersonalisierung** oder der **Direktwerbung** gestattet.²⁰¹
- 247 Zum anderen muss die **Verarbeitung für die genannten Zwecke** der Vertragserfüllung beziehungsweise der Durchführung vorvertraglicher Maßnahmen **erforderlich** sein. Im Rahmen des Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO bedeutet dies, dass die betreffende Verarbeitung **objektiv erforderlicher Vertragsbestandteil** sein muss im Sinne eines unmittelbaren sachlichen Zusammenhangs zwischen der beabsichtigten Datenverarbeitung und dem konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses.²⁰² Die bloße Erwähnung einer Datenverarbeitung in einem Vertrag oder deren Nützlichkeit für die Erfüllung eines Vertrags genügen dagegen nicht.
- 248 Diese Erforderlichkeit muss auch das für die Datenverarbeitung konkret eingesetzte **Betriebsmittel**, beispielsweise ein KI-System, **umfassen**. Insbesondere muss dessen Einsatz

¹⁹⁹ Vergleiche im Einzelnen Buchner/Petri, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 6 DSGVO Rn. 33.

²⁰⁰ Vergleiche im Einzelnen Buchner/Petri, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 6 DSGVO Rn. 32a.

²⁰¹ Buchner/Petri, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 6 DSGVO Rn. 37.

²⁰² Vergleiche im Einzelnen Buchner/Petri, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 6 DSGVO Rn. 33, 39.

3. Datenschutzrechtliche Anforderungen

aus der Perspektive der betroffenen Person als Bestandteil für die Vertragserfüllung voraussehbar und müssen dessen Zwecke eindeutig sein.

In der Regel sind danach weder das initiale Training eines KI-Systems noch dessen Weitertraining objektiv erforderliche Haupt- oder Nebenpflichten eines (vor-)vertraglichen Schuldverhältnisses im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO, es sei denn, das KI-Training ist selbst Vertragsgegenstand. 249

Schwieriger ist die Beurteilung, wenn KI-Systeme unterstützend bei der Erbringung vertraglicher Leistungen in unterschiedlichem Intensitäts- oder Wirkungsgrad genutzt werden, beispielsweise beim Einsatz von Chatbots im Rahmen eines Bürgerportals. Hier ist eine Beurteilung im Einzelfall erforderlich, inwieweit die Datenverarbeitung mittels KI-Systems objektiv erforderlich ist. 250

ee) Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO)

Für **Notlagen hinsichtlich des Schutzes von lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person**, beispielsweise im Fall einer konkreten Gefahr für die körperliche Unversehrtheit und das Leben, statuiert Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO eine **subsidiäre (EG 46 Satz 2 DSGVO)** Rechtsgrundlage für Verarbeitungen personenbezogener Daten. Mit Blick auf den Ausnahmecharakter der Norm muss für deren Anwendbarkeit eine unmittelbare Bedrohung im Sinne einer **konkreten Gefahr** in einer kurzfristigen Notsituation für lebenswichtige Interessen natürlicher Personen bestehen; auch darf **kein milderes, gleich effektives Mittel** als die betreffende Verarbeitung personenbezogener Daten in Betracht kommen. Der Erlaubnistatbestand des Schutzes lebenswichtiger Interessen umfasst **keine allgemeine Vorsorge** zur Abwehr lebensbedrohlicher Risiken. 251

Aus diesem Grund kommt der Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. d DSGVO in der Praxis nur geringe Bedeutung zu. Im Zusammenhang mit **KI-Systemen** ist eine ein (in der Regel zeitaufwendiges) **KI-Training** erforderlich machende **Notsituation schon nicht vorstellbar**; grundsätzlich denkbar wäre dagegen im Einzelfall der Einsatz eines KI-Systems beispielsweise im Zusammenhang mit **Notfallrettung**, wobei insoweit zudem die Voraussetzungen des Art. 9 DSGVO zu beachten wären. 252

ff) Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)

Für Verarbeitungen von besonderen Kategorien personenbezogener Daten im Sinne von **Art. 9 Abs. 1 in Verbindung mit Art. 4 Nr. 13 bis 15 DSGVO** gelten gesteigerte datenschutzrechtliche Schutzanforderungen. Aufgrund deren Sensibilität und den mit ihrer Verarbeitung verbundenen **erheblichen Risiken für die Grundrechte und Grundfreiheiten** der betroffenen Personen ist deren **Verarbeitung grundsätzlich verboten** und nur **ausnahmsweise unter den engen Voraussetzungen des Art. 9 Abs. 2 bis 4 DSGVO** erlaubt. Zu beachten ist dabei, dass die Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO **nur dann** 253

V. Datenschutz-Grundverordnung

rechtmäßig ist, wenn neben den Vorgaben des Art. 9 Abs. 2 bis 4 DSGVO auch **mindestens eine der in Art. 6 Abs. 1 DSGVO genannten Rechtmäßigkeitsvoraussetzungen erfüllt** ist.²⁰³

- 254 Art. 9 DSGVO ist anwendbar, wenn **besonders sensible personenbezogene Daten** verarbeitet werden. Dazu zählen nach Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten (Art. 4 Nr. 13 DSGVO), biometrischen Daten (Art. 4 Nr. 14 DSGVO) zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
- 255 Eine Verarbeitung kann darauf angelegt sein, besonders sensible Daten zu verarbeiten. Besonders sensible Daten können sich aber auch nur **mittelbar** aus dem Gesamtzusammenhang einer Verarbeitung ergeben oder überhaupt **erst durch eine solche Verarbeitung** entstehen. Letztere Möglichkeit besteht aufgrund der großen Mengen an Datensätzen und der Vielzahl an Kombinationsmöglichkeiten im KI-Kontext in besonderem Maße – zusätzlich zur mit Blick auf die Datenmengen häufig auftretenden unmittelbaren Verarbeitung besonderer Kategorien personenbezogener Daten.

Beispiele: Bei der Beantragung eines Parkausweises, der zum Parken auf Schwerbehindertparkplätzen berechtigt, wird das Vorliegen bestimmter gesundheitlicher Einschränkungen als Voraussetzung für dessen Erteilung abgefragt. Eine entsprechende amtliche Bescheinigung²⁰⁴ ist regelmäßig vorzulegen. Setzt eine Kommune ein KI-System ein, das Angaben der Bescheinigung mit den Voraussetzungen für einen derartigen Parkausweis abgleicht, werden hierbei Gesundheitsdaten der Antragsteller im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet.

Erst durch die Verarbeitung einzelner (personenbezogener) Daten entstehen besondere Kategorien personenbezogener Daten beispielsweise dann, wenn ein bei der Antragstellung auf freiwillige Leistungen der Ausländerbehörde eingesetztes KI-System eine Plausibilitätsprüfung der Angaben des Antragstellers vornimmt (und hierbei etwa sein Aufenthalt in einer psychiatrischen Klinik offenbart wird).

- 256 Doch nicht jede Datenverarbeitung im KI-Kontext führt zwangsläufig zu einer Verarbeitung personenbezogener Daten und der Anwendbarkeit von Art. 9 DSGVO²⁰⁵. Der **Zweck der Datenverarbeitung spielt bei der Einordnung eine entscheidende Rolle**: Wird ein KI-System zur Verarbeitung besonderer Datenkategorien eingesetzt oder zielt es auf deren Gewinnung, gilt Art. 9 DSGVO mit dessen zusätzlichen Anforderungen an die Rechtmäßigkeit der Datenverarbeitung (neben solchen aus Art. 6 DSGVO). Anders ist der Fall zu bewerten, in dem besonders sensible Daten – trotz aller Vorkehrungen des Verantwortlichen – „zufällig“ in die zu verarbeitenden Datenmengen gelangen, die Verarbeitung vom Verantwortlichen aber nicht intendiert ist.

²⁰³ EuGH, Urteil vom 21. Dezember 2023, C-667/21, Rn. 79.

²⁰⁴ Bescheinigung des Zentrums Bayern Familie und Soziales (ZBFS).

²⁰⁵ So für den Fall der Videoüberwachung bereits EDSA, Leitlinien 3/2019 zur „Verarbeitung personenbezogener Daten durch Videogeräte“, Version 2.0, Stand 1/2020, Rn. 62 f., Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de.

3. Datenschutzrechtliche Anforderungen

Die Anwendung von Art. 9 DSGVO kann gleichwohl nicht alleine dadurch vermieden werden, dass verantwortliche Stellen die zielgerichtete Verarbeitung besonderer Datenkategorien einfach abstreiten. Bei KI-Systemen, die in der Regel äußerst große Mengen – Verantwortlichen im Einzelnen unbekannter – Daten verarbeiten, ist naheliegend, dass in dem Datensatz stets (etwa mittelbar entstandene) besonders sensible Kategorien personenbezogener Daten enthalten sind. **Ist keine Verarbeitung besonderer Datenkategorien beabsichtigt, muss der Verantwortliche – beispielsweise durch technisch-organisatorische Maßnahmen – dafür Sorge tragen, dass eine solche Verarbeitung auch tatsächlich möglichst ausgeschlossen bleibt.** Diese Anforderung erwächst aus dem Grundsatz der Datenminimierung (siehe Rn. 206 f.). 257

Dies stellt die verantwortlichen öffentlichen Stellen, die ein KI-System – eine entsprechende Rechtsgrundlage vorausgesetzt – trainieren oder nutzen wollen, vor zusätzliche Herausforderungen: sie müssen im Vorfeld der von ihnen beabsichtigten Datenverarbeitungen sorgfältig **bewerten, welche Datenverarbeitungen unter Berücksichtigung der Lern-, Arbeits- und Weiterentwicklungsprozesse des jeweiligen KI-Systems stattfinden werden und ob auf dieser Grundlage potenziell mittelbar oder unmittelbar neue und/oder besonders sensible Datensätze entstehen** können. Diese Einschätzung ist nicht nur für die Frage der Rechtmäßigkeit der einzelnen Verarbeitungsvorgänge von Bedeutung; nach ihr richten sich auch die Maßnahmen, die es zu ergreifen gilt, um das Risiko der Verletzung der Rechte und Freiheiten der betroffenen Personen zu minimieren. Um die Prognoseentscheidung zu vereinfachen, erscheint es für die Verantwortlichen empfehlenswert, sich an dem höchstmöglichen Risiko zu orientieren und möglichst hohe Schutzmechanismen vorzusehen. Hierbei gilt: je größer die Datenmenge und je unbekannter die Datenquellen, desto höher ist die Wahrscheinlichkeit für das Vorhandensein und die Entstehung von besonders sensiblen Datenkategorien bei der beabsichtigten Datenverarbeitung. 258

Abweichend vom grundsätzlichen Verbot des Art. 9 Abs. 1 DSGVO ermöglichen die **Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO** eine Verarbeitung besonderer Kategorien personenbezogener Daten. Hierzu zählen unter anderem die **ausdrückliche Einwilligung** der betroffenen Person (Art. 9 Abs. 2 Buchst. a DSGVO), der **Schutz lebenswichtiger Interessen** natürlicher Personen (Art. 9 Abs. 2 Buchst. b DSGVO mit der zusätzlichen Einschränkung, dass die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande sein muss, ihre Einwilligung zu geben; zum beschränkten Anwendungsbereich dieses Tatbestands siehe oben Rn. 251 f.), eine **offensichtliche Öffentlichmachung der Daten durch die betroffene Person** (Art. 9 Abs. 2 Buchst. e DSGVO) sowie die Verarbeitung aus **Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit** (Art. 9 Abs. 2 Buchst. i DSGVO) oder **zu im öffentlichen Interesse liegenden Archiv-, Forschungs- oder statistischen Zwecken** (Art. 9 Abs. 2 Buchst. j DSGVO). 259

(1) Einwilligung (Art. 9 Abs. 2 Buchst. a DSGVO)

Für die Wirksamkeit der Einwilligung der betroffenen Personen in die Verarbeitung ihrer personenbezogenen Daten besonderer Kategorien nach Art. 9 Abs. 2 Buchst. a DSGVO gelten **grundsätzlich dieselben Anforderungen wie an eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO**, siehe oben Rn. 230 ff., wobei Art. 9 Abs. 2 Buchst. a DSGVO als **zusätzliche** Voraussetzung die **Ausdrücklichkeit** der Einwilligung fordert. 260

V. Datenschutz-Grundverordnung

- 261 Die verantwortlichen Stellen haben bei Datenverarbeitungen mittels Künstlicher Intelligenz auf der Grundlage von Einwilligungen stets die damit einhergehenden Besonderheiten und Einschränkungen zu beachten (vgl. Rn. 231 ff.). So wird etwa das Training eines KI-Systems mit besonderen Kategorien personenbezogener Daten auf der Grundlage von Einwilligungen im Sinne von Art. 9 Abs. 2 Buchst. a DSGVO wegen der Vielzahl an benötigten Einwilligungen der betroffenen Personen (und deren Widerruflichkeit) nicht praktikabel sein, siehe auch unter Rn. 241.

(2) Veröffentlichung durch die betroffene Person (Art. 9 Abs. 2 Buchst. e DSGVO)

- 262 Im Zusammenhang mit dem Training von KI-Systemen mit **im Internet verfügbaren Daten** könnte der in Art. 9 Abs. 2 Buchst. e DSGVO normierten Ausnahme größere Bedeutung zukommen. Danach gilt das Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO nicht für solche personenbezogenen Daten, die die **betroffene Person offensichtlich öffentlich gemacht** hat.
- 263 **Öffentlich** sind Daten im Sinne von Art. 9 Abs. 2 Buchst. e DSGVO dann, wenn sie **einem unbestimmten Personenkreis zugänglich** gemacht werden. Dies trifft typischerweise auf die Veröffentlichung der Daten im **Internet** zu. Für die Ausnahme des Art. 9 Abs. 2 Buchst. e DSGVO genügt jedoch nicht, dass die personenbezogenen Daten allgemein zugänglich sind; vielmehr muss diese öffentliche Zugänglichkeit auf einer **bewussten Entscheidung** der betroffenen Person im Sinne einer **Zurechenbarkeit** beruhen.²⁰⁶
- 264 Die solche öffentlichen Daten verwendenden Stellen sind als **Verantwortliche** für das Vorliegen der vorgenannten Voraussetzungen, insbesondere der bewussten Öffentlichmachung durch die betroffene Person, **nach Art. 5 Abs. 2 DSGVO nachweispflichtig**. In Zweifelsfällen – etwa bei Internetveröffentlichungen mit unklarer Herkunft – darf nicht automatisch angenommen werden, dass die betroffene Person ihre Daten öffentlich gemacht hat. Um diese Problematik zu vermeiden beziehungsweise zu entschärfen, sollten die Verantwortlichen bereits im Vorfeld eine **gezielte Auswahl von zu verwendenden Datenquellen** treffen. Dies kann beispielsweise durch Verzicht auf die Datenerhebung von bestimmten (Teilen von) Websites oder durch die Berücksichtigung von Privatsphäre-Einstellungen von Internet-Portalen (etwa durch Login geschützte Bereiche) im Rahmen des Web-Crawlings geschehen. Technisch setzt dies voraus, dass Websites entsprechend konfiguriert sind (etwa mittels robots.txt-Datei oder über Meta-Tags im HTML-Header). Auch aus diesem Grund sind zusätzlich (wirksame) Filterungsmaßnahmen, wie URL-Filter, oder Einschränkungen des Crawl-Bereichs empfehlenswert. Bei kleineren beschränkten Datenbeständen ist eine solche Kategorisierung dagegen einfacher umsetzbar.

²⁰⁶ Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, Art. 9 DSGVO Rn. 57. Vgl. auch EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 77 ff., wonach personenbezogene Daten offenkundig öffentlich gemacht werden, wenn eine Person ausdrücklich und durch eine eindeutige und bestätigende Handlung beabsichtigt, die betreffenden personenbezogenen Daten der Öffentlichkeit zugänglich zu machen. Kann die Person Einstellungen betreffend ihre Daten vornehmen und weiß sie, dass ihre Informationen von der Allgemeinheit oder einer begrenzten Anzahl von Personen eingesehen werden können, und entscheidet sie sich ausdrücklich dafür, ihre Informationen zu veröffentlichen, dann hat die Person ihre Informationen offenkundig öffentlich gemacht.

(3) Archiv-, Forschungs- oder statistische Zwecke (Art. 9 Abs. 2 Buchst. j DSGVO)

Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten für **im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke** richtet sich – auch bei Einsatz von KI-Systemen – nach Art. 9 Abs. 2 Buchst. j DSGVO, dessen Anforderungen **durch Art. 89 Abs. 1 DSGVO** (und in dessen nationalrechtlicher Ausgestaltung durch **Art. 25 und Art. 26 BayDSG**²⁰⁷) **konkretisiert** werden. Die Regelung des Art. 9 Abs. 2 Buchst. j DSGVO ist auf die Privilegierung dieser Zwecke aufgrund deren hohen gesamtgesellschaftlichen Rangs zurückzuführen, die unter anderem auch in Art. 5 Abs. 1 Buchst. b Halbsatz 2 DSGVO mit Blick auf den Grundsatz der Zweckkompatibilität ihren Niederschlag findet. 265

So setzt die Rechtmäßigkeit der Verarbeitung neben der Verfolgung der genannten Zwecke voraus, dass diese auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erfolgt, das den Wesensgehalt des Rechts auf Datenschutz wahrt und überdies angemessene und spezifische Schutzmaßnahmen vorsieht. Berücksichtigungsfähige Kriterien können insoweit etwa die Bedeutung des jeweiligen Zwecks für die Allgemeinheit, die Tiefe der Grundrechtseingriffe für die Betroffenen sowie die ihnen gebotenen Garantien sein. Insbesondere muss geprüft werden, inwieweit die Verarbeitungszwecke auch ohne personenbezogene Daten oder mit zumindest pseudonymisierten Daten erreicht werden können (vgl. EG 156 DSGVO).²⁰⁸ 266

(4) Art. 9 Abs. 2 Buchst. g DSGVO in Verbindung mit Art. 10 Abs. 5 KI-Verordnung

Für Trainings-, Test- und Validierungsdaten von Hochrisiko-KI-Systemen enthält Art. 10 Abs. 5 KI-Verordnung – wie gesehen (Rn. 126) in Ausformung des Regelungsspielraums des Art. 9 Abs. 2 Buchst. g in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 Buchst. a DSGVO – eine Rechtsgrundlage für die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO zur Vermeidung von Bias, das heißt, soweit die Datenverarbeitung für die Erkennung und Korrektur von Verzerrungen innerhalb von Hochrisiko-KI-Systemen unbedingt erforderlich ist. Allerdings sind in diesem Fall angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen zu treffen. Die KI-Verordnung statuiert zusätzliche Rechtmäßigkeitsbedingungen. 267

(5) Zweckänderung (Art. 6 Abs. 4 DSGVO, Art. 6 Abs. 2 BayDSG)

Da sich Datenverarbeitungszwecke gerade im Bereich der Künstlichen Intelligenz bei der Erhebung personenbezogener Daten oftmals noch nicht klar benennen lassen oder sich aufgrund des der Künstlichen Intelligenz immanenten Lern- und Entwicklungsprozesses ändern, kommt den gesetzlichen Vorgaben zur Zweckänderung insoweit besondere Bedeutung zu. So sieht der **Grundsatz der Zweckbindung in Art. 5 Abs. 1 Buchst. b Halbsatz 1 DSGVO** prinzipiell vor, dass personenbezogene Daten nicht in einer mit den festgelegten, eindeutigen und legitimen Zwecken der betreffenden Verarbeitung nicht zu vereinbarenden Weise 268

²⁰⁷ Bayerischer Landtag, LT-Drs. 17/19628, S. 44 f.

²⁰⁸ Petri, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2. Aufl. 2025, Art. 9 DSGVO Rn. 96.

V. Datenschutz-Grundverordnung

weiterverarbeitet werden dürfen. Ausnahmen hiervon sind nur im Rahmen der sogenannten „Forschungsausnahme“ (Art. 5 Abs. 1 Buchst. b Halbsatz 2 in Verbindung mit Art. 89 Abs. 1 DSGVO) sowie unter bestimmten Voraussetzungen nach **Art. 6 Abs. 4 DSGVO** vorgesehen.

- 269 Danach ist gemäß **Art. 6 Abs. 4 Var. 2 DSGVO** eine Zweckänderung der Verarbeitung personenbezogener Daten insbesondere dann möglich, wenn sie auf einer **Rechtsvorschrift der Union oder der Mitgliedstaaten** beruht, die in einer demokratischen Gesellschaft eine **notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele** darstellt.
- 270 Für die Weiterverarbeitung personenbezogener Daten zu anderen als den Erhebungszwecken durch bayerische **öffentliche Stellen** enthält **Art. 6 Abs. 2 BayDSG** eine nationalrechtliche Regelung in diesem Sinne. **Art. 6 Abs. 2 BayDSG** nennt neun mögliche Zweckänderungstatbestände „unbeschadet der Bestimmungen der [Datenschutz-Grundverordnung]“, wobei im Zusammenhang mit **KI-Systemen** insbesondere **Art. 6 Abs. 2 Nr. 2 BayDSG** – die Daten können aus allgemein zugänglichen Quellen entnommen werden oder die Daten verarbeitende Stelle dürfte sie veröffentlichen – und **Art. 6 Abs. 2 Nr. 3 Buchst. c BayDSG** – Erforderlichkeit der Verarbeitung zur Durchführung wissenschaftlicher oder historischer Forschung unter Interessenabwägung²⁰⁹ und Betrachtung der Zweckerreichung – als Zweckänderungsbefugnisse in Betracht kommen könnten. **Unberührt** hiervon bleibt gemäß **Art. 6 Abs. 3 BayDSG** am Ende die nach **Art. 24 Abs. 3 BayDSG** bestehende **Zweckbindung bei der Videoüberwachung**. Weiterhin enthält **Art. 6 Abs. 4 BayDSG** ein **Weiterverarbeitungsverbot** für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung und der Datenschutzkontrolle verarbeitet werden.
- 271 Eine Rechtsvorschrift des Unionsrechts im Sinne von **Art. 6 Abs. 4 Var. 2 DSGVO** enthält **Art. 59 KI-Verordnung** (zweckändernde Nutzung von personenbezogenen Daten in **Real-laboren**, Näheres hierzu unter Rn. 126 ff.).
- 272 Nach **Art. 6 Abs. 4 Var. 1 DSGVO** kann eine zweckändernde Weiterverarbeitung auch auf eine **Einwilligung** der betroffenen Person gestützt werden, wobei diese den oben unter Rn. 231 ff. beschriebenen Voraussetzungen und Einschränkungen unterliegt.
- 273 Für die Anwendung des „Kompatibilitätstests“ des **Art. 6 Abs. 4 Var. 3 DSGVO** als Auffangtatbestand bleibt aufgrund der Einschlägigkeit der vorrangigen nationalrechtlich abschließenden Regelung des Art. 6 Abs. 2 BayDSG für öffentliche Stellen **kein Raum**.
- 274 Liegt eine Zweckänderungsbefugnis vor, sind in Bezug auf die zweckändernde Weiterverarbeitung **sämtliche datenschutzrechtlichen Grundsätze** einzuhalten und werden insbesondere **Informationspflichten** durch eine Zweckänderung **erneut ausgelöst**.

c) Datenschutzrechtliche Verantwortlichkeit

- 275 Die für die Verarbeitung von personenbezogenen Daten verantwortliche Stelle ist **zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet** und muss diese **im**

²⁰⁹ Vgl. hierzu Niese, in: Wilde/Ehmann/Niese/Knoblach, Datenschutz in Bayern, Bayerisches Datenschutzgesetz, Datenschutzgrundverordnung, Art. 6 BayDSG Rn. 33.

3. Datenschutzrechtliche Anforderungen

Rahmen ihrer Rechenschaftspflicht nachweisen können, Art. 5 Abs. 2 DSGVO.²¹⁰ Art und Umfang der Anforderungen richten sich maßgeblich nach der Rollenverteilung der Beteiligten bei den Verarbeitungsvorgängen.

Im Zusammenhang mit der Nutzung von KI-Systemen sind regelmäßig mehrere Akteure an verschiedenen Verarbeitungsvorgängen beteiligt. Nicht nur aus Sicht der von der Verarbeitung betroffenen Personen ist es daher besonders relevant, die Rollen der Beteiligten vorab erfahren zu können; es ist auch im Interesse der (potenziell) Verantwortlichen, die Frage der Rollenverteilung rechtzeitig vor Aufnahme einer Verarbeitungstätigkeit zu klären. 276

Bei der Einordnung der Akteure in das Rollenmodell der Datenschutz-Grundverordnung ist zunächst darauf zu achten, dass die **einzelnen Verarbeitungsvorgänge differenziert** zu betrachten sind. So kann ein und dieselbe Stelle im Zusammenhang mit der Entwicklung und dem Training eines KI-Systems eine andere Rolle einnehmen als im Zusammenhang mit dessen Nutzung. Zudem können sich die Verantwortlichkeiten für einzelne Verarbeitungsvorgänge **im Laufe der Zeit ändern**²¹¹ und/oder sich – beispielsweise bei großen Unternehmensgeflechten – **überschneiden**. 277

Beispiel: Ein Anbieter trainiert ein KI-System mit personenbezogenen Daten, um es zu vermarkten (alleinige Verantwortlichkeit des Anbieters). Anschließend wird das KI-System vom Anbieter als Cloud-Lösung zur eigenverantwortlichen Nutzung durch Dritte, das heißt Betreiber, angeboten (in der Regel Auftragsverarbeitung mit dem Betreiber als datenschutzrechtlich Verantwortlichem und dem Anbieter als Auftragsverarbeiter).

Das **Rollenmodell der Datenschutz-Grundverordnung** ist **abschließend**. Der nationale Gesetzgeber kann keine neuen Rollen „dazuerfinden“. Die Einordnung und Abgrenzung können im Einzelfall Schwierigkeiten bereiten.²¹² Zu unterscheiden sind die im Folgenden dargestellten Rollen. 278

Hinweis: Das datenschutzrechtliche Rollenmodell ist ein **funktionelles Konzept eigener Prägung**. Es zielt darauf ab, Verantwortlichkeiten entsprechend den tatsächlichen Gegebenheiten und unabhängig von einer formellen Benennung oder (vertraglichen) Festlegung zuzuweisen (funktionelles Konzept),²¹³ wobei die Rollenmerkmale durch das unionale Datenschutzrecht vorgegeben sind (Konzept eigener Prägung). 279

aa) Alleinige Verantwortlichkeit

Verantwortlicher ist nach **Art. 4 Nr. 7 Halbsatz 1 DSGVO** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff der Verantwortlichkeit wird generell **weit** verstanden, um einen wirksamen und umfassenden 280

²¹⁰ Hierzu siehe auch oben Rn. 134.

²¹¹ Siehe in diesem Zusammenhang Art. 7 Abs. 2 Buchst. c Richtlinie (EU) 2024/2853, wonach die Haftung des Verantwortlichen auf nach der Implementierung entstandene Fehler ausgedehnt wird.

²¹² Zur Abgrenzung der verschiedenen Rollen der Datenschutz-Grundverordnung vergleiche Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit, Orientierungshilfe, Stand 6/2024, Rn. 89 ff., Internet: <https://www.datenschutz-bayern.de/infothek/>.

²¹³ Schlussanträge des Generalanwalts Emiliou vom 4. Mai 2023 in der Rechtssache C-683/21, Rn. 41.

V. Datenschutz-Grundverordnung

Schutz der betroffenen Personen zu gewährleisten. Jede Person, „die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt“, das heißt einen Beitrag zur Entscheidung leistet, ist als Verantwortlicher anzusehen.²¹⁴ Dabei ist zu beachten: Der Zugriff auf die betreffenden verarbeitungsgegenständlichen Daten gewährt allein noch keine Kontrolle im Sinne einer Verantwortung. Ebenso wenig sind eine eigene Verarbeitung personenbezogener Daten²¹⁵ oder der Zugang zu den Daten Voraussetzungen für die Einstufung als für die Verarbeitung Verantwortlicher.²¹⁶ Maßgeblich ist vielmehr die Entscheidungsbefugnis²¹⁷ in Bezug auf die wesentlichen Aspekte der Verarbeitung, wozu der Zweck sowie die wesentlichen Mittel²¹⁸ gehören. Besteht – wie typischerweise bei Beschäftigten (siehe Art. 29 DSGVO) – keine solche Entscheidungsbefugnis, ist auch eine datenschutzrechtliche Verantwortlichkeit zu verneinen (Nichtverantwortlichkeit).

- 281 **Hinweis:** Das Bayerische Datenschutzgesetz enthält auf der Grundlage von Art. 4 Nr. 7 Halbsatz 2 DSGVO in **Art. 3 Abs. 2 BayDSG** eine Konkretisierung dahin, dass **Verantwortlicher für die Verarbeitung personenbezogener Daten** im Sinne der Datenschutz-Grundverordnung im Anwendungsbereich des Bayerischen Datenschutzgesetzes **die für die Verarbeitung zuständige öffentliche Stelle ist, soweit nichts anderes bestimmt** ist. Dabei ergibt sich die Bestimmung der **bayerischen öffentlichen Stellen** grundsätzlich aus **Art. 1 BayDSG**. Spezialgesetze können abweichende Regelungen treffen.²¹⁹

Beispiel für Alleinverantwortlichkeit (bezogen auf die Phase des Einsatzes und der Nutzung eines KI-Systems): Erwerb und Einsatz eines vollständig austrainierten KI-Systems bei einer öffentlichen Stelle ausschließlich zu eigenen Zwecken auf eigenen Servern.

- 282 Der **Anbieter** eines KI-Systems ist **in der Regel der datenschutzrechtlich Verantwortliche** für die Verarbeitungstätigkeiten, die er zur **Entwicklung und zum Training** dieses KI-Systems durchgeführt hat, da er deren Zweck und die hierfür eingesetzten Mittel festlegt. Dies gilt nicht nur für einen Anbieter, der ein KI-System auf der Grundlage eines selbst erhobenen Trainingsdatensatzes entwickelt, sondern auch für einen Anbieter, der die Erhebung eines solchen Trainingsdatensatzes mittels hinreichend detaillierter dokumentierter Anweisungen

²¹⁴ EuGH, Urteil vom 10. Juli 2018, C-25/17, Rn. 68.

²¹⁵ EuGH, Urteil vom 5. Dezember 2023, C-683/21, Rn. 35.

²¹⁶ EuGH, Urteil vom 10. Juli 2018, C-25/17, Rn. 69. In diesem Sinne auch EuGH, Urteil vom 5. Juni 2018, C-210/16, Rn. 38.

²¹⁷ Für diese Entscheidungsbefugnis sind in der Praxis verschiedene Grundlagen denkbar, welche in einem Stufenverhältnis zueinander stehen: (1) Entscheidungsbefugnis kraft Rechtsvorschriften, (2) Entscheidungsbefugnis aufgrund einer implizierten Zuständigkeit sowie (3) subsidiär: tatsächlicher Einfluss. Näher hierzu Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212), Rn. 23 ff.

²¹⁸ Im Rahmen einer Auftragsverarbeitung kann es insoweit einen gewissen Spielraum für den Auftragsverarbeiter geben, eigenständige Entscheidungen in Bezug auf die nicht wesentlichen Mittel einer Verarbeitung zu treffen, vergleiche Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212), Rn. 45.

²¹⁹ Siehe nur § 67 Abs. 4 Zehntes Buch Sozialgesetzbuch - Sozialverfahren und Sozialdatenschutz -, § 69 Satz 2 Bundespersonalvertretungsgesetz, § 27 Satz 1 Gesetz zur Durchführung des Zensus im Jahr 2022 sowie Art. 1 Satz 2 Gesetz zur Ausführung des Personenstandsgesetzes.

3. Datenschutzrechtliche Anforderungen

einem Dienstleister überlässt (welcher insoweit datenschutzrechtlich als Auftragsverarbeiter fungiert).

Datenschutzrechtlich verantwortlich für die Verarbeitung personenbezogener Daten im Zusammenhang mit der **Nutzung** eines KI-Systems ist regelmäßig dessen **Betreiber**, da dieser in der Regel bestimmt, zu welchem Zweck und mit welchen Daten er ein bestimmtes KI-System einsetzt.

283

Im Zusammenhang mit dem Betrieb von KI-Systemen ist zudem die Regelung zum sogenannten „**Quasi-Anbieter**“ in **Art. 25 KI-Verordnung** zu beachten: Nach Art. 25 Abs. 1 Buchst. c KI-Verordnung gelten insbesondere Betreiber, die die Zweckbestimmung eines KI-Systems, das nicht als hochriskant eingestuft und bereits in den Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System im Sinne von Art. 6 KI-Verordnung wird, für die Zwecke der KI-Verordnung als Anbieter eines Hochrisiko-KI-Systems. Eine solche Änderung der Zweckbestimmung würde gleichzeitig den Gegenstand und gegebenenfalls die Reichweite der datenschutzrechtlichen Verantwortlichkeit und der damit verbundenen Rechte und Pflichten des Betreibers eines KI-Systems verändern.

284

Beispiele: Ein Anbieter bietet einen KI-basierten Sprachassistenten, der nicht als hochriskant eingestuft wurde, als KI-as-a-Service zur Nutzung am Markt an. Bei Verarbeitung personenbezogener Daten wird der Anbieter des Sprachassistenten insoweit datenschutzrechtlich als Auftragsverarbeiter des nutzenden Betreibers als dem Verantwortlichen tätig.

Setzt der Betreiber des Sprachassistenten diesen zu einem hochriskanten Zweck ein, geht die Anbieterrolle mit allen daran anknüpfenden Pflichten insoweit auf ihn über (vgl. Art. 25 Abs. 2 Satz 1 KI-Verordnung). Durch die Ausweitung der Datenverarbeitungsvorgänge erweitert sich zudem die datenschutzrechtliche Verantwortlichkeit des verantwortlichen Betreibers und nun Quasi-Anbieters. Der Erstanbieter ist nach Art. 25 Abs. 2 Satz 2 KI-Verordnung in diesem Fall verpflichtet, eng mit dem neuen Anbieter zusammenzuarbeiten, ihm die erforderlichen Informationen zur Verfügung zu stellen und für den vernünftigerweise zu erwartenden technischen Zugang und die sonstige Unterstützung zu sorgen, die für die Erfüllung der in der KI-Verordnung festgelegten Pflichten erforderlich sind.

Diese Unterstützungspflicht gilt gemäß Art. 25 Abs. 2 Satz 3 KI-Verordnung nicht, wenn der Anbieter des als KI-as-a-Service angebotenen KI-basierten Sprachassistenten dessen Einsatz zu hochriskanten Zwecken im Sinne des Art. 6 KI-Verordnung – beispielsweise in seinen Nutzungsbedingungen und Lizenzverträgen – ausschließt und der Betreiber den Sprachassistenten entgegen der Vorgaben des Anbieters doch zu einem hochriskanten Zweck einsetzt. Zudem könnte der Anbieter als Auftragsverarbeiter aufgrund der eindeutig anderslautenden Nutzungsbedingungen und Lizenzverträge die Ausführung der Weisungen des Betreibers verweigern.

bb) Gemeinsame Verantwortlichkeit

Nach **Art. 26 Abs. 1 Satz 1 DSGVO** ist gemeinsam verantwortlich, wer zusammen mit mindestens einem anderen Verantwortlichen „die Zwecke der und die Mittel zur Verarbeitung“

285

V. Datenschutz-Grundverordnung

personenbezogener Daten festlegt.²²⁰ Die gemeinsame Verantwortlichkeit zeichnet sich danach vor allem dadurch aus, dass jeder der Beteiligten „Herr über die Verarbeitung“ ist: Jeder der gemeinsam Verantwortlichen ist in der Lage, auf den Verarbeitungsvorgang, das heißt das von definierten Beweggründen getragene, erwartete und beabsichtigte Ergebnis („Warum“ = Zweck), und die Art und Weise, dieses Ergebnis zu erreichen („Wie“ = Mittel), steuernd einzuwirken.²²¹ Die Entscheidungen müssen dabei gemeinsam getroffen werden oder zumindest konvergierend, allerdings nicht gleichberechtigt oder einstimmig sein.²²² Daraus folgt nach der Rechtsprechung des Europäischen Gerichtshofs,²²³ dass eine rein faktische Zusammenarbeit für gleiche oder ähnliche Zwecke im Eigeninteresse ausreichend ist. Eine bloße Mitursächlichkeit für eine Verarbeitung personenbezogener Daten genügt dagegen nicht.

286 Liegt eine gemeinsame Verantwortlichkeit vor, statuiert **Art. 26 Abs. 1 Satz 2 DSGVO** als Rechtsfolge die **Verpflichtung zum Abschluss einer Vereinbarung**. In dieser müssen die Beteiligten in transparenter Form festlegen, wer von ihnen welche datenschutzrechtlichen Verpflichtungen gemäß der Datenschutz-Grundverordnung erfüllt.²²⁴ Eine besondere Bedeutung kommt hierbei der Wahrnehmung der Rechte der betroffenen Person sowie der Erfüllung der Informationspflichten gemäß Art. 13 und Art. 14 DSGVO zu (Art. 26 Abs. 1 Satz 2 DSGVO am Ende). Für die betroffenen Personen soll auch bei der Zusammenarbeit von mehreren Beteiligten einfach erkennbar sein, wer für welchen Verarbeitungsvorgang hinsichtlich ihrer personenbezogenen Daten verantwortlich ist (vgl. EG 79 DSGVO). Nach **Art. 26 Abs. 3 DSGVO** können sie ihre Rechte allerdings – unabhängig von den Regelungen der Vereinbarung – bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

287 In diesem Zusammenhang ist zu beachten, dass die Erfüllung der Tatbestandsmerkmale des Art. 26 DSGVO und damit die Begründung einer gemeinsamen Verantwortlichkeit **keine Rechtsgrundlage für die in gemeinsamer Verantwortlichkeit durchgeführten Datenverarbeitungen** darstellt. Vielmehr benötigt jeder der Verantwortlichen eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO für die Verarbeitung personenbezogener Daten im Rahmen der gemeinsamen Verantwortlichkeit; bei der Verarbeitung besonderer Kategorien personenbezogener Daten zusätzlich nach Maßgabe von Art. 9 Abs. 2 DSGVO.²²⁵ Einer solchen Rechtsgrundlage bedarf es **auch für die Datenübermittlung der gemeinsam Verantwortlichen untereinander** – mangels gesonderter Rechtspersönlichkeit der gemeinsam Verantwortlichen sind diese Empfänger im Sinne des Art. 4 Nr. 9 DSGVO, soweit die gemeinsame

²²⁰ Zur gemeinsamen Verantwortlichkeit umfassend Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212).

²²¹ Martini, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 26 DSGVO Rn. 19.

²²² Hierzu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212), Rn. 56 ff.; EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, Stand 7/2021, Rn. 55, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de.

²²³ Vergleiche EuGH, Urteil vom 5. Juni 2018, C-210/16, sowie Urteil vom 10. Juli 2018, C-25/17.

²²⁴ Zum Inhalt der Vereinbarung ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212), Rn. 141 ff.

²²⁵ Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212), Rn. 122 f. Zu den Rechtsgrundlagen siehe oben Rn. 216 ff.

3. Datenschutzrechtliche Anforderungen

Verantwortlichkeit reicht, und genießen – im Gegensatz zum Auftragsverhältnis – kein Verarbeitungsprivileg.²²⁶

Beispiele für gemeinsame Verantwortlichkeit: Zwei eigenständige verantwortliche Stellen nehmen an einem gemeinsamen Projekt teil, dessen Gegenstand es ist, ein KI-System mit gemeinsamen Datensätzen zu trainieren, um im Anschluss das trainierte KI-System zu eigenen Zwecken (etwa zur Behandlung eigener Patienten) zu nutzen. Beim Training agieren die Beteiligten als gemeinsam Verantwortliche. Die anschließende Verwendung geschieht regelmäßig jeweils alleinverantwortlich.

Eine gemeinsame Verantwortlichkeit kann wiederum vorliegen, soweit in diesem Fall ein gemeinsames Weitertraining des KI-Systems aufgrund neuer Datensätze erfolgt. Dies gilt je nach Einzelfall auch dann, wenn der Betreiber eines KI-Systems gegenüber dessen Anbieter die Nutzung seiner Eingabedaten zu (Weiter-)Trainingszwecken erlaubt.

cc) Auftragsverarbeitung

Besonders bei arbeitsteiligen mehrstufigen Datenverarbeitungsprozessen ist auch an die datenschutzrechtliche Figur der Auftragsverarbeitung nach **Art. 4 Nr. 8, Art. 28 und Art. 29 DSGVO** zu denken. Gemäß Art. 4 Nr. 8 DSGVO ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.²²⁷ Die beauftragte (eigenständige) Stelle muss also weisungsgebunden personenbezogene Daten für den beauftragenden Verantwortlichen (und nicht für eigene Zwecke) verarbeiten (vgl. Art. 29, Art. 28 Abs. 10 DSGVO). 288

Externe KI-Systeme einsetzende öffentliche Stellen müssen daher darauf achten, Anbietern **nicht** – gegebenenfalls aus Versehen – vertraglich **das Recht einzuräumen, die in das System eingegebenen Daten für das weitere Training oder für sonstige eigene Zwecke verwenden** zu dürfen. 289

Bei der **Auswahl** des Auftragsverarbeiters hat die verantwortliche Stelle zu beachten, dass sie gemäß **Art. 28 Abs. 1 DSGVO** nur solche Stellen mit der Verarbeitung personenbezogener Daten beauftragen darf, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung steht und der Schutz der Rechte der betroffenen Person gewährleistet ist. 290

Bei der Nutzung von KI-Systemen ist in diesem Zusammenhang ein besonderes Augenmerk darauf zu richten, ob der Anbieter des betreffenden Systems die genannten Anforderungen einhalten kann. Insbesondere kann zu prüfen sein, ob er entsprechend auf das KI-System einwirken kann. 291

²²⁶ Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit (Fn. 212), Rn. 124 ff. mit Hinweis auf den Sonderfall der Rechtsstellung als Dritte im Sinne des Art. 4 Nr. 10 DSGVO, wenn einer der gemeinsam Verantwortlichen seinen Sitz in einem Drittland hat.

²²⁷ Zur Auftragsverarbeitung umfassend Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, Internet: <https://www.datenschutz-bayern.de/infothek/>.

V. Datenschutz-Grundverordnung

- 292 Zudem sind Konfigurationsmöglichkeiten der als Dienstleistungen beauftragten Datenverarbeitungen sowie vertragliche Ausgestaltungsmöglichkeiten (etwa hinsichtlich des Umfangs der Informationspflichten, Einwilligungserklärungen usw.) zu nutzen.
- 293 Das Auftragsverarbeitungsverhältnis ist nach **Art. 28 Abs. 3 Satz 1 DSGVO** durch einen **Vertrag oder ein anderes Rechtsinstrument** zu regeln, wobei zwingend die Mindestanforderungen des Art. 28 Abs. 3 DSGVO zu erfüllen sind.²²⁸
- 294 Liegt ein Auftragsverarbeitungsverhältnis in diesem Sinne vor, leitet sich die Rechtmäßigkeit von Verarbeitungen personenbezogener Daten in diesem Rahmen aus der **Rechtsgrundlage** ab, **auf die der Verantwortliche selbst die betreffende Verarbeitung personenbezogener Daten stützt**. Für die Weitergabe der verarbeitungsgegenständlichen personenbezogenen Daten vom Verantwortlichen an den Auftragsverarbeiter sowie die Verarbeitung durch diesen ist regelmäßig keine weitere Rechtsgrundlage erforderlich (**Privilegierung der Auftragsverarbeitung**).²²⁹

Beispiele für Auftragsverarbeitung:

- Weitertraining eines KI-Systems durch einen Dienstleister als Auftragsverarbeiter auf Weisung und mit personenbezogenen Datenbeständen der das KI-System einsetzenden öffentlichen Stelle als Verantwortlichem, eine entsprechende Rechtsgrundlage vorausgesetzt;
- Nutzung eines von einem Dienstleister vollständig austrainierten und im Rahmen eines Auftragsverarbeitungsverhältnisses als Cloud-Lösung angebotenen KI-Systems in eigener Verantwortung einer öffentlichen Stelle als Verantwortlichem. Dies gilt jedoch nur unter der Voraussetzung, dass die Eingaben personenbezogener Daten von einzelnen Nutzern nicht zum Weitertraining des KI-Systems oder zu anderen eigenen Zwecken des Anbieters genutzt werden. Im Fall einer Weiternutzung kommen je nach Einzelfall eine gemeinsame Verantwortlichkeit oder jeweils Einzelverantwortlichkeiten in Betracht.

- 295 **Handlungsempfehlung:** Öffentliche Stellen sollten die Frage der datenschutzrechtlichen Verantwortlichkeiten rechtzeitig vor der Entwicklung, der Implementierung und der Nutzung von KI-Systemen klären. Hierbei ist eine klare **Abgrenzung der Rollen**, von gemeinsamen und individuellen Verarbeitungszwecken sowie von gemeinsamen und unabhängigen Entscheidungen **wichtig**. Maßgeblich sind insoweit die tatsächlichen Umstände des Einzelfalls unter Berücksichtigung der an den unterschiedlichen Verarbeitungsvorgängen beteiligten Akteure.

d) Weitere datenschutzrechtliche Aspekte

aa) Informationspflichten (Art. 12 ff. DSGVO)

- 296 Die für eine Verarbeitung personenbezogener Daten verantwortlichen Stellen haben dafür Sorge zu tragen, dass sie den Informationspflichten nach Art. 12 ff. DSGVO als Ausformung des **Transparenzgrundsatzes des Art. 5 Abs. 1 Buchst. a DSGVO** nachkommen

²²⁸ Im Einzelnen hierzu Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung (Fn. 227), S. 15 ff.

²²⁹ Vergleiche Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung (Fn. 227), S. 7.

3. Datenschutzrechtliche Anforderungen

(können).²³⁰ So verpflichtet **Art. 12 Abs. 1 Satz 1 DSGVO** den Verantwortlichen unter anderem dazu, geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen gemäß den Art. 13 und Art. 14 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (vgl. hierzu auch **EG 58 DSGVO**).

Der **Umfang der Informationen** richtet sich nach Art. 13 und Art. 14 DSGVO, wobei **Art. 13 DSGVO für direkte Datenerhebungen** bei den betroffenen Personen anwendbar ist, während die Informationspflicht des **Art. 14 DSGVO** für sonstige Datenzuflüsse, etwa bei Dritten, gilt.

Die jeweils zur Verfügung zu stellenden **Informationen decken sich dabei großteils**. Betreffend Datenverarbeitungen mittels **Künstlicher Intelligenz** kommt insoweit den Informationspflichten zu **Verarbeitungszwecken** (Art. 13 Abs. 1 Buchst. c DSGVO, Art. 14 Abs. 1 Buchst. c DSGVO), zu **(Kategorien von) Empfängern** (Art. 13 Abs. 1 Buchst. e DSGVO, Art. 14 Abs. 1 Buchst. e DSGVO) sowie gegebenenfalls zum **Bestehen einer automatisierten Entscheidungsfindung** (Art. 13 Abs. 2 Buchst. f DSGVO, Art. 14 Abs. 2 Buchst. g DSGVO, hierzu unten Rn. 337) **besondere Bedeutung** zu. Der **Detaillierungsgrad** der Informationen ist gesetzlich nicht beschrieben. Er muss in einem angemessenen Verhältnis zu dem von der Verarbeitung ausgehenden Risiko stehen; dabei gilt: je größer das von einer Verarbeitung ausgehende Risiko, desto mehr Transparenz für die betroffenen Personen.

Praxishinweis: Insbesondere die **Informationspflicht zu Verarbeitungszwecken** nach Art. 13 Abs. 1 Buchst. c DSGVO, Art. 14 Abs. 1 Buchst. c DSGVO soll die betroffene Person in die Lage versetzen, **Anlass und Umfang der Verarbeitung ihrer personenbezogenen Daten zu überblicken**. Aus diesem Grund wird **empfohlen**, mit Blick auf die Risiken von Datenverarbeitungen mittels Künstlicher Intelligenz die betroffenen Personen **auch hinsichtlich der „Form der Verarbeitung“ und des hierfür eingesetzten Betriebsmittels „KI-System“** zu informieren, vgl. EG 60 Satz 2 DSGVO.²³¹

Hierzu gehören beispielsweise Informationen zur Entwicklung und Bewertung, zu den Funktionalitäten, den Trainingsdaten (Kategorien, Quelle, Metadaten), den beabsichtigten Einsatzmöglichkeiten, den Leistungskennzahlen sowie den Schutzmaßnahmen und Einschränkungen des eingesetzten KI-Systems.

Nach **Art. 14 Abs. 1 Buchst. d DSGVO** sind zudem die **verarbeiteten Datenkategorien** mitzuteilen, einschließlich ihrer **Quelle**, **Art. 14 Abs. 2 Buchst. f DSGVO**.

Diese Verpflichtungen stellen die Verantwortlichen aufgrund der **Komplexität und oftmals Intransparenz von KI-Systemen** im Einzelfall vor **Herausforderungen** und müssen

²³⁰ Zu den Informationspflichten im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortlichen, Orientierungshilfe, Stand 11/2018, Internet: <https://www.datenschutz-bayern.de/infotehk/>.

²³¹ So auch DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Dezember 2025, DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich (Fn. 93), S. 2. Ablehnend Bortnikov, Transparenz bei KI-Systemen, DuD 2025, S. 297, 298. Zu einem umfassenden Open-Government-Ansatz in Form eines nationalen KI-Transparenzregisters als „Bringschuld“ des Staates“ Botta, Ein KI-Transparenzregister für die öffentliche Verwaltung, Die Verwaltung 58 (2025), S. 139, 142 ff.

V. Datenschutz-Grundverordnung

insbesondere **beim Erwerb und Einsatz von extern austrainierten KI-Systemen** bedacht werden, beispielsweise durch vertragliche Vereinbarung von **Unterstützungspflichten** durch den Entwickler oder Anbieter des betreffenden Systems. Zur inhaltlichen Ausformung können die Vorgaben des Europäischen Gerichtshofs in der Rechtssache „Dun & Bradstreet Austria“ herangezogen werden (hierzu näher unten Rn. 338).²³² Das Urteil erging zwar zum Auskunftsanspruch nach Art. 15 Abs. 1 Buchst. h in Verbindung mit Art. 22 DSGVO, kann aber auch für die Erfüllung der Vorgaben der Art. 13 Abs. 2 Buchst. f, Art. 14 Abs. 2 Buchst. g DSGVO fruchtbar gemacht werden, da die genannten Informationspflichten eine Einheit mit dem korrespondierenden Auskunftsanspruch bilden.²³³

302 **Praxishinweise:** Die Herausforderungen aufgrund von Komplexität und oftmals Intransparenz von KI-Systemen wirken sich gegebenenfalls auch auf die **Feststellung von Verletzungen des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO** und den Umgang mit diesen, insbesondere hinsichtlich der **Melde- und Benachrichtigungspflichten nach Art. 33 und Art. 34 DSGVO**, aus:

- So kann zum einen die **technische Komplexität** von Künstlicher Intelligenz die **Nachvollziehbarkeit von deren Funktionsweise beeinträchtigen**. Fehlt Verantwortlichen das nötige technische Verständnis, sind sie nicht nur außerstande zu beurteilen, ob das betreffende KI-System ordnungsgemäß funktioniert, sondern erschwert dies auch die Risikoeinschätzung im Einzelfall. Die Feststellung, ob überhaupt eine Verletzung der Sicherheit und damit eine meldepflichtige Datenschutzverletzung vorliegt, kann somit in der Praxis herausfordernd sein.
- Besonders bei arbeitsteiligen mehrstufigen Datenverarbeitungsprozessen mittels Künstlicher Intelligenz kann die Einordnung und Abgrenzung von (Nicht-)Verantwortlichkeiten im Einzelfall nicht unerhebliche Schwierigkeiten bereiten.
- Schließlich ist auch die Wahrung der kurzen Melde- und Benachrichtigungsfristen im Zusammenhang mit Künstlicher Intelligenz aufgrund deren Komplexität zumindest erschwert. In der Praxis hilfreich ist insoweit die Regelung des Art. 33 Abs. 4 DSGVO, der ein schrittweises Vorgehen zulässt, wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können.

Auch die **KI-Verordnung kennt Melde- und Benachrichtigungspflichten**, namentlich für **„KI-Systeme, die ein Risiko bergen“ im Sinne des Art. 79 KI-Verordnung**, beispielsweise nach Art. 20 Abs. 2, Art. 24 Abs. 2 Satz 2 und Abs. 4 Satz 2, Art. 26 Abs. 5 Satz 2 KI-Verordnung. So verpflichtet **Art. 26 Abs. 5 Satz 2 KI-Verordnung** zum Beispiel den Betreiber eines Hochrisiko-KI-Systems dazu, unverzüglich den Anbieter oder Händler und die zuständige Marktüberwachungsbehörde zu informieren und die Verwendung des Hochrisiko-KI-Systems auszusetzen, wenn er Grund zu der Annahme hat, dass die Verwendung des Hochrisiko-KI-Systems gemäß der Betriebsanleitung dazu führen kann, dass das System ein Risiko im Sinne des Art. 79 Abs. 1 KI-Verordnung birgt.

303 Bei **(späteren) Zweckänderungen durch den zu diesem Zeitpunkt Verantwortlichen** – beispielsweise der Weiterverarbeitung von Eingabedaten zum Weitertraining eines KI-Systems – leben die Informationspflichten **wieder auf, Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO**.

²³² EuGH, Urteil vom 27. Februar 2025, C-203/22.

²³³ EuGH, Urteil vom 7. Dezember 2023, C-634/21 (SCHUFA).

3. Datenschutzrechtliche Anforderungen

In **zeitlicher Hinsicht** statuiert Art. 13 DSGVO, dass „zum Zeitpunkt der Erhebung“ zu informieren ist, während Art. 14 Abs. 3 DSGVO gestaffelte Fristen vorsieht, innerhalb welcher der Verantwortliche seiner Informationspflicht nachkommen muss. 304

Teilweise unterschiedlich geregelt sind zudem die **Ausschlusstatbestände**, bei deren Vorliegen eine Informationspflicht nicht besteht: So sind die verantwortlichen Stellen nach **Art. 13 Abs. 4, Art. 14 Abs. 5 Buchst. a DSGVO** von der Pflicht zur Erteilung der Informationen **befreit, wenn und soweit die betroffene Person bereits über die Informationen verfügt**. 305

Gemäß **Art. 14 Abs. 5 Buchst. b Satz 1 Halbsatz 1 DSGVO** entfällt die Verpflichtung zur Information zudem, wenn sich **die Erteilung dieser Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern** würde. Der Begriff des „unverhältnismäßigen Aufwands“ wird dabei nicht definiert. Mit Blick auf die Regelbeispiele in Art. 14 Abs. 5 Buchst. b Satz 1 Halbsatz 2 DSGVO sowie die Interpretation der Artikel 29-Datenschutzgruppe²³⁴ kann diese Ausnahme allerdings nur in **sehr engen Grenzen** Anwendung finden, beispielsweise bei einer großen Zahl an betroffenen Personen und eventuellen Schwierigkeiten bei deren Ermittlung. Der Verantwortliche muss also **vorab den entstehenden Aufwand mit den Informationsinteressen der betroffenen Personen** abwägen. Er kann dabei unter anderem berücksichtigen, ob die betreffenden Daten bereits vorher öffentlich zugänglich waren. 306

Praxishinweis: (Massenhafte) Datenverarbeitungen durch KI-Systeme könnten daher durchaus zum denkbaren Anwendungsbereich des Ausnahmetatbestands des Art. 14 Abs. 5 Buchst. b Satz 1 Halbsatz 1 DSGVO zählen. 307

Möchte sich eine verantwortliche Stelle auf Art. 14 Abs. 5 Buchst. b DSGVO berufen, muss sie dessen **Voraussetzungen durch entsprechende Dokumentation nachweisen**²³⁵ und **zusätzlich geeignete Maßnahmen** zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergreifen, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit (**Art. 14 Abs. 5 Buchst. b Satz 2 DSGVO**). 308

Neben diesen Informationspflichten sind beim Einsatz von KI-Systemen zusätzlich die jeweils einschlägigen **Transparenzpflichten nach der KI-Verordnung** zu erfüllen (siehe oben Rn. 55 ff.). 309

bb) Betroffenenrechte

Im **Gegengewicht** zu den Rechten des Verantwortlichen, personenbezogene Daten zu verarbeiten, **gewährleisten Art. 15 ff. DSGVO die Rechte der betroffenen Person**, insbesondere das Recht auf Auskunft (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO) und das Recht auf Löschung (Art. 17 DSGVO), und ermöglichen es der betroffenen Person, die **Kontrolle über ihre Daten zu behalten**. Die für die Datenverarbeitung verantwortlichen 310

²³⁴ Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, Stand 4/2018, S. 38, Internet: <https://www.datenschutz-bayern.de/infothek/>: Verwendung einer Datenbank mit Nachnamen von über 20.000 Betroffenen zu Forschungszwecken, wobei die Daten seit deren Erhebung 50 Jahre zuvor nicht aktualisiert wurden und keinerlei Kontaktinformation enthalten.

²³⁵ Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (Fn. 234), S. 39.

V. Datenschutz-Grundverordnung

Stellen sind nicht nur gesetzlich verpflichtet, die Betroffenenrechte zu erfüllen, sondern sie haben auch sicherzustellen, dass betroffene Personen ihre Rechte nach Art. 15 ff. DSGVO wirksam ausüben können.

- 311** Öffentliche Stellen, welche die Entwicklung oder den Einsatz von **KI-Systemen** planen, müssen sich daher über die Gewährleistung der Betroffenenrechte sowohl hinsichtlich des KI-Systems als Ganzem als auch hinsichtlich der jeweils zugrundeliegenden KI-Modelle²³⁶ frühzeitig Gedanken machen. So ist unter anderem zu klären, ob möglicherweise bereits bestehende Prozesse zur Bearbeitung von Anträgen betroffener Personen nach Art. 15 ff. DSGVO auch für Datenverarbeitungen im Zusammenhang mit KI-Systemen geeignet und praktikabel sind. Gegebenenfalls müssen neue technische und organisatorische Maßnahmen zur effizienten Umsetzung der Betroffenenrechte entwickelt und implementiert werden. Werden KI-Systeme oder -Modelle externer Anbieter genutzt, sind die einsetzenden Stellen je nach Einzelfall auf entsprechende **Unterstützung durch die Entwickler und/oder Anbieter**, beispielsweise in Form von (umfassenden) Dokumentationen, angewiesen. Eine entsprechende Unterstützungspflicht, auch betreffend die Erfüllung der Betroffenenrechte, ergibt sich im Fall einer Auftragsverarbeitung ausdrücklich aus **Art. 28 Abs. 3 Satz 2 Buchst. e DSGVO**, kann aber auch individualvertraglich vereinbart werden.
- 312** Die Etablierung transparenter, effizienter und gleichförmiger Prozesse zur Umsetzung der Betroffenenrechte erleichtert es auch, die **Fristvorgabe des Art. 12 Abs. 3 Satz 1 DSGVO** zu erfüllen, wonach der Verantwortliche den betroffenen Personen grundsätzlich **innerhalb eines Monats** Informationen über die auf Antrag gemäß den Art. 15 bis Art. 22 DSGVO ergriffenen Maßnahmen zur Verfügung stellen muss.

(1) Recht auf Auskunft (Art. 15 DSGVO)

- 313** Gemäß Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht auf Auskunft über die von dem Verantwortlichen verarbeiteten sie betreffenden personenbezogenen Daten sowie über die Informationen nach Art. 15 Abs. 1 Buchst. a bis h DSGVO.²³⁷ Für betroffene Personen hat dieses Recht die Funktion eines „**Schlüsselrechts**“, wenn sie die nötigen Informationen erlangen möchten, um die Rechtmäßigkeit einer Verarbeitung einschätzen und/oder Betroffenenrechte ausüben zu können.
- 314** Für die Verantwortlichen dürfte die Erfüllung des Auskunftsrechts im KI-Kontext regelmäßig mit neuen Herausforderungen verbunden sein. So kann sich bereits die Beantwortung der Frage, ob die betreffenden personenbezogenen Daten der Antragsteller verarbeitet werden, als schwierig erweisen. Dies gilt insbesondere mit Blick auf die Trainingsdaten für den Fall, in dem externe KI-Systeme genutzt werden. Verantwortliche, die solche KI-Systeme nutzen, sollten im Falle eines Auskunftersuchens die ihnen zur Verfügung stehenden und vernünftigerweise zu erwartenden Mittel zur Ermittlung nutzen, ob personenbezogene Daten der

²³⁶ Dagegen für einen Fokus auf die Systemebene Fuchs/Wünschelbaum/Hansen/Walczak, The Bridge Blueprint. Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim KI-Einsatz (Fn. 122), S. 5.

²³⁷ Ausführlich hierzu Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 12/2019, Internet: <https://www.datenschutz-bayern.de/infotehk/>.

3. Datenschutzrechtliche Anforderungen

auskunftssuchenden Person bei Nutzung des KI-Systems (weiter)verarbeitet werden. Hier- von ist allerdings atypisches Einwirken auf das System, beispielsweise mittels „Membership Interference Attacks“ oder „Model Inversion Attacks“, nicht umfasst.

Praxishinweis: Bei Beauskunftung von in **Großen Sprachmodellen** verarbeiteten perso- 315 nenbezogenen Daten kann eine Abfrage beispielsweise über einen entsprechenden **Prompt** („Was weißt Du über [Name]?“ oder „Schreibe alle Informationen zu [Name].“) hilfreich sein.

Liegen die Anspruchsvoraussetzungen des Art. 15 Abs. 1 Halbsatz 1 DSGVO vor, muss der 316 Verantwortliche neben einer Bestätigung der Verarbeitung personenbezogener Daten des Antragstellers **die weiteren in Art. 15 Abs. 1 Buchst. a bis h DSGVO genannten Informa- tionen** zur Verfügung stellen. Auch dies setzt voraus, dass er **Kenntnis über die dem Aus- kunftsanspruch gegenständlichen Daten** hat.

Beim Training von KI-Systemen mit **eigenen Datenbeständen** beziehungsweise der **Nut- 317 zung selbst trainierter KI-Systeme** ist die Feststellung der vom Auskunftsrecht betroffenen Daten, jedenfalls betreffend Datenverarbeitungen im Rahmen des Trainings, häufig unprob- lematish.²³⁸ Für die Ermittlung der Datensätze der auskunftersuchenden Person aus **späte- ren Verarbeitungsphasen** ist neben der **Arbeitsweise** des jeweiligen KI-Systems dessen **Ausgestaltung als abgeschottetes oder offenes System entscheidend**. So wird bei allge- mein zugänglichen offenen Systemen, wie beispielsweise Cloud-Lösungen, der vollständige Datensatz einer bestimmten Person kaum ausfindig gemacht werden können. Diese Proble- matik wird beim **Einsatz von externen KI-Systemen** noch weiter verschärft: Der **einsetzen- den Stelle** werden mangels Einblicks in das System und dessen Training regelmäßig nicht alle dem Auskunftsanspruch nach Art. 15 Abs. 1 Buchst. a bis h DSGVO unterliegenden Infor- mationen vorliegen.

Auch insoweit sind Verantwortliche je nach Einzelfall auf entsprechende **Unterstützung 318 durch die Entwickler und/oder Anbieter des genutzten KI-Systems** angewiesen und sollten dies vertraglich absichern. Für **Anbieter von KI-Modellen mit allgemeinem Ver- wendungszweck** verlangt **Art. 53 Abs. 1 Buchst. a in Verbindung mit Anhang XI Ab- schnitt 1 Nr. 2 Buchst. c KI-Verordnung** sogar ausdrücklich, dass sie **Informationen über die für das Trainieren, Testen und Validieren verwendeten Daten** bereitstellen, „ein- schließlich der Art und Herkunft der Daten und der Aufbereitungsmethoden (zum Beispiel Bereinigung, Filterung usw.), der Zahl der Datenpunkte, ihres Umfangs und ihrer Hauptmerk- male, gegebenenfalls [über] die Art und Weise, wie die Daten erlangt und ausgewählt wurden, sowie [über] alle anderen Maßnahmen zur Feststellung, ob Datenquellen ungeeignet sind, und Methoden zur Erkennung unmittelbarer Verzerrungen“. Zudem sind sie nach **Art. 53 Abs. 1 Buchst. b in Verbindung mit Anhang XII KI-Verordnung** verpflichtet, den Anbie- tern von KI-Systemen, die beabsichtigen, das KI-Modell mit allgemeinem Verwendungs- zweck in ihre KI-Systeme zu integrieren (sogenannte „nachgelagerte Anbieter“, Art. 3 Nr. 68 KI-Verordnung), **Informationen und Dokumentation** zur Verfügung zu stellen und aktuell zu halten, **um die Fähigkeiten und Grenzen des KI-Modells mit allgemeinem**

²³⁸ Verfahren der Datenkuratierung und Datenherkunft.

V. Datenschutz-Grundverordnung

Verwendungszweck gut zu verstehen und den Pflichten gemäß der KI-Verordnung nachzukommen.²³⁹

319 **Praxishinweis:** Bei Datenverarbeitungen im Zusammenhang mit der Nutzung von KI-Systemen kann es aus diesem Grund **im Einzelfall ratsam** sein, die **Eingaben und die Ausgabeberechnungen** zu protokollieren. Die **Speicherung** dieser Protokollierung muss jedoch **zeitlich begrenzt** sein, und die Eingebenden sind auf die Speicherung **hinzuweisen**. Derartige Protokolle unterliegen im Übrigen ihrerseits den Verarbeitungsgrundsätzen und insbesondere dem Auskunftsrecht.

320 Für den Fall, dass der Verantwortliche **nachweislich** nicht in der Lage ist, die betroffene Person zu (re-)identifizieren, kommt die Ausnahme des **Art. 11 Abs. 2 Satz 2 DSGVO** in Betracht, der Art. 15 bis Art. 20 DSGVO ausnahmsweise für nicht anwendbar erklärt. Soweit externe KI-Systeme genutzt werden, die auf Großen Sprachmodellen beruhen, dürften sich Verantwortliche grundsätzlich auf diese Ausnahme berufen können – jedenfalls mit Blick auf die Trainingsdaten des KI-Systems. Die in Art. 11 Abs. 2 Satz 2 DSGVO vorgesehene Rücknahme, dass die betroffene Person zusätzliche Informationen bereitstellt, die ihre Identifizierung ermöglichen, dürfte in dem vorgenannten Fall fernliegend sein.

321 Für die Inanspruchnahme des Art. 11 Abs. 2 DSGVO ist es allerdings **nicht ausreichend, dass der Verantwortliche den Aufwand einer für ihn möglichen Identifizierung scheut oder die fehlende Identifizierbarkeit einfach behauptet**.²⁴⁰ Alle möglichen und zumutbaren Vorkehrungen zur (Re-)Identifizierung sind bereits bei der Gestaltung der Verarbeitung nach Art. 24, Art. 25 und Art. 32 DSGVO zu treffen (siehe unter Rn. 343 ff.) und im Falle eines Auskunftersuchens anzuwenden. Nur wenn diese zu keinem „Treffer“ bei der Ermittlung entsprechender Daten führen, darf sich die Daten verarbeitende Stelle auf Art. 11 Abs. 2 DSGVO berufen. In diesem Fall ist **die auskunftssuchende Person hierüber zu unterrichten**, Art. 11 Abs. 2 Satz 1 DSGVO.

(2) Recht auf Berichtigung (Art. 16 DSGVO) und Recht auf Löschung (Art. 17 DSGVO)

322 Das Recht auf Berichtigung (Art. 16 DSGVO) und das Recht auf Löschung (Art. 17 DSGVO)²⁴¹ eröffnen betroffenen Personen die Möglichkeit, auf „ihren“ Datenbestand bei einem Verantwortlichen Einfluss zu nehmen und so über die weitere Verarbeitung mitzubestimmen. Sie statuieren jeweils ein **subjektives Recht der betroffenen Person**, dem eine entsprechende **objektive Pflicht des Verantwortlichen** gegenübersteht.

323 Während das Recht auf Berichtigung nach **Art. 16 DSGVO** auf der **Tatbestandsebene eine objektive Unrichtigkeit personenbezogener Daten**²⁴² voraussetzt, knüpft **Art. 17 DSGVO**

²³⁹ Zum Verhältnis von Art. 53 Abs. 1 Buchst. c zu Art. 25 Abs. 4 KI-Verordnung Siesing-Wagenpfeil, GPAI-Modelle in der Wertschöpfungskette der KI-VO, DuD 2025, S. 225, 229 f.

²⁴⁰ Hansen, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2. Aufl. 2025, Art. 11 DSGVO Rn. 32.

²⁴¹ Zum Recht auf Löschung umfassend Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 6/2022, Internet: <https://www.datenschutz-bayern.de/infothek/>.

²⁴² Hierzu siehe bereits Rn. 208 ff. zum Grundsatz der Datenrichtigkeit.

3. Datenschutzrechtliche Anforderungen

an die in Art. 17 Abs. 1 Buchst. a bis f DSGVO aufgezählten Lösungsgründe an. **Art. 17 Abs. 3 DSGVO** enthält **Ausnahmen**.

Beide Rechte müssen auch beim Einsatz von **KI-Systemen** gewährleistet werden. Aufgrund der oftmals komplexen Ausgestaltung dieser Systeme ist **für die Ermittlung der jeweils zu ergreifenden Maßnahmen des Verantwortlichen** als Adressat der Betroffenenrechte eine sorgfältig **nach Verarbeitungsvorgängen getrennte Betrachtung** unter Berücksichtigung des **Standes der Technik und der Wissenschaft** erforderlich. Sind bestimmte Maßnahmen technisch (noch) nicht umsetzbar, darf deren Kompensation allerdings nur zeitlich begrenzt erfolgen und muss gegebenenfalls durch dem Stand der Wissenschaft entsprechende Maßnahmen ausgeglichen werden; sobald geeignete technische und organisatorische Maßnahmen existieren, ist die Lösung mit dem geringsten Eingriff in die Rechte der betroffenen Personen umzusetzen.

324

Beispiel: Die **Trainingsdaten eines vollständig austrainierten KI-Systems**, das von einer öffentlichen Stelle zum eigenverantwortlichen Betrieb auf eigenen Servern erworben wird, liegen **außerhalb des Einwirkungs- und damit Verantwortungsbereichs der öffentlichen Stelle**. Ein **Berichtigungsanspruch**, der sich auf diese Trainingsdaten bezieht, kann allein durch die für das Training verantwortliche Stelle, in der Regel den **Hersteller** und/oder **Anbieter**, erfüllt werden. Deren Mitwirkung in bestimmten Fällen sollte der Verantwortliche daher möglichst vertraglich absichern. Die öffentliche Stelle als Betreiber des KI-Systems ist dagegen für eine etwaige Weiterverarbeitung der – mitunter aus dem Training stammenden – unrichtigen Daten verantwortlich und ist im Hinblick darauf der Adressat der Betroffenenrechte. Als datenschutzrechtlich Verantwortlicher für ein von ihr als Betriebsmittel eingesetztes KI-System muss sie dessen datenschutzkonforme Nutzung sicherstellen und nachweisen (Art. 5 Abs. 2 DSGVO). Dies umfasst auf der Grundlage einer Einzelfallbetrachtung (Rn. 169) **auch die Frage der Rechtmäßigkeit des vorhergehenden Trainings und dessen Auswirkungen auf die Rechtmäßigkeit der Nutzung** des betreffenden Systems. Den Verantwortlichen trifft insoweit eine einzelfallspezifische, aufsichtsbehördlich überprüfbare Pflicht zur „angemessenen Bewertung“.²⁴³

So kann eine Berichtigung unrichtiger Daten im Sinne von **Art. 16 Satz 1 DSGVO** im Zusammenhang mit einem KI-System, abhängig von der Phase der Datenverarbeitung und der Fehlerquelle, etwa durch eine **bloße Korrektur der Ausgabedaten** (beispielsweise bei nutzerbedingt unrichtiger Eingabe) umgesetzt werden oder gar ein **umfängliches Nachtraining** erfordern (zum Beispiel bei Verwendung unrichtiger Eingaben oder Ergebnisse zum Weitertraining des KI-Systems).

325

Auch die Erfüllung der Löschpflicht nach **Art. 17 DSGVO** im Zusammenhang mit KI-Systemen kann einzelfallabhängig auf unterschiedlichen Wegen erfolgen.²⁴⁴ Es ist jedoch

326

²⁴³ EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Fn. 146), Rn. 122, 126, 128 ff.

²⁴⁴ Vgl. zu Korrekturmöglichkeiten zum Beispiel Werry, Generative KI-Modelle im Visier der Datenschutzbehörden, Technische Entwicklungen im Zusammenhang mit KI-Modellen begegnen einer Vielzahl datenschutzrechtlicher Herausforderungen, MMR 2023, S. 911, 914. Siehe des Weiteren auch die von noyb am 29. April 2024 eingereichte Beschwerde gegen OpenAI nach Ablehnung eines Antrags auf Berichtigung oder Löschung (wegen eines falsch ausgegebenen Geburtsdatums), Internet: <https://noyb.eu/de/chatgpt-provides-false->

V. Datenschutz-Grundverordnung

erforderlich, dass **nicht nur die Ausgabe** der zu löschenden Daten durch beispielsweise Filtertechnologien²⁴⁵ verhindert wird, sondern dass die betreffenden Daten **dauerhaft gelöscht** werden **oder** zumindest ein datenschutzkonformes „**Löschäquivalent**“²⁴⁶ vorliegt, mittels welchem die betreffenden Daten unumkehrbar unkenntlich gemacht werden, sodass deren (Weiter-)Verarbeitung nicht oder nur mit unververtretbarem Aufwand möglich ist.²⁴⁷ Insoweit ist zu beachten, dass einige KI-Systeme gegebenenfalls erst durch Verknüpfung unterschiedlicher Daten einen Personenbezug herstellen können. Daher ist ein besonderes Augenmerk darauf zu richten, dass die zur Löschung getroffenen Maßnahmen eine **Wiederherstellung des Personenbezugs dauerhaft unmöglich** machen. Die **zielgerichtete Löschung** einzelner personenbezogener Daten aus einem KI-System ist dabei **oftmals nur schwer oder nur mit unverhältnismäßigem Aufwand** möglich und/oder **beeinträchtigt dessen Funktionsfähigkeit**. Aus diesem Grund werden Methoden des „Entlernens“ („**Unlearning**“)²⁴⁸ oder „Wiederlernens“ („**ReLearn**“)²⁴⁹ entwickelt, mit deren Hilfe alte und fehlerhafte Daten **zielgerichtet aus Systemen entfernt** oder die **Wahrscheinlichkeit einer Ausgabe** des betreffenden personenbezogenen Datums **reduziert** werden sollen. Zudem kann die Löschpflicht auch durch eine **unumkehrbare Anonymisierung** oder durch **wirksame Zugriffsbeschränkungen** im Rahmen eines Rechte- und Rollenkonzepts erfüllt werden. In Einzelfällen können schließlich sogar ein **vollständiger Austausch der Datensätze** und ein **Neutraining** notwendig sein.

- 327 In der Praxis können Berichtigungs- und Löschanträge – je nach Art und Nutzung eines KI-Systems – die verantwortlichen Stellen aber durchaus an **technische Grenzen** bringen. Denn viele, insbesondere generative, KI-Systeme sind möglicherweise gar nicht in der Lage, Daten zu „vergessen“, oder eine Einwirkung auf die dem System zugrundeliegenden Daten hat im Einzelfall (weitreichende) Auswirkungen auf die Funktionsfähigkeit des KI-Systems

information-about-people-and-openai-cant-correct-it, sowie https://noyb.eu/sites/default/files/2024-04/OpenAI%20Complaint_DE_geschw%C3%A4rzt.pdf.

²⁴⁵ Solche Filtertechnologien, die bestimmte unerwünschte Ausgaben unterdrücken, können zwar einen Beitrag zur Wahrung der Datenschutzrechte leisten, siehe DSK, Künstliche Intelligenz und Datenschutz (Fn. 170), S. 8. Gleichwohl sind sie als alleinige Maßnahme nicht geeignet, eine Löschung im Sinne von Art. 17 DSGVO zu bewirken.

²⁴⁶ Vgl. DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Dezember 2025, DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich (Fn. 93), S. 2.

²⁴⁷ Vgl. Peuker, in: Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. 2022, Art. 17 DSGVO, Rn. 32.; Herbst, in: Kühling/Buchner, DSGVO / BDSG, 4. Aufl. 2024, Art. 17 DSGVO Rn. 37.

²⁴⁸ Eine Übersicht über Literatur zum Thema „Machine Unlearning“ findet sich unter https://github.com/jjbrophy47/machine_unlearning. Siehe auch International Working Group on Data Protection in Technology, Working Paper on Large Language Models (LLMs) (Fn. 143), S. 55 f., und Shrishak, Effective implementation of data subjects' rights, EDSA Support Pool of Experts Programme, S. 5 ff. mit Differenzierung von Methoden des „exact unlearning“ und des „approximate unlearning“ und Hinweis auf Bedenken im Zusammenhang mit „machine unlearning“ (S. 8 f.), Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-complex-algorithms-and-effective-data_en. Zu „influence-guided machine unlearning“ vgl. Fan/Wu/Zhou/Liang/Phung, IMU: Influence-guided Machine Unlearning, arXiv:2025.01620, Internet: <https://www.arxiv.org/abs/2508.01620>.

²⁴⁹ „ReLearn“ soll mittels Datenanreicherung und Feinabstimmung ein effektiveres Verlernen als „Unlearning“ ermöglichen. Hierzu umfassend Xu et al., ReLearn: Unlearning via Learning for Large Language Models, arXiv:2502.11190, Internet: <https://arxiv.org/abs/2502.11190>.

3. Datenschutzrechtliche Anforderungen

insgesamt.²⁵⁰ Bei Einsatz und Nutzung solcher (externer) Systeme ist daher **besondere Vorsicht** geboten.

Handlungsempfehlung: Die verantwortlichen Stellen haben vor der Entwicklung und/oder Nutzung eines KI-Systems sicherzustellen, dass technische Möglichkeiten für eine Berichtigung von unrichtigen oder unrichtig gewordenen Daten und für die Löschung von Daten vorhanden und umsetzbar sind, etwa durch Einsatz von KI-Systemen, die zum „Unlearning“ oder „ReLearn“ fähig sind. Dies gilt auch vor dem Hintergrund, dass die Verarbeitung von personenbezogenen Daten regelmäßig einer Speicherfrist unterliegt, nach deren Ablauf sie (ohne Antrag nach Art. 17 DSGVO) zu löschen sind. 328

cc) Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO)

Bereits bei Konzeption von KI-basierten Systemen ist zu bedenken, dass diese grundsätzlich **keine menschliche Entscheidung mit Rechtswirkung ersetzen** dürfen: Gemäß Art. 22 Abs. 1 DSGVO haben betroffene Personen das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung, einschließlich Profiling (Art. 4 Nr. 4 DSGVO),²⁵¹ unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Vielmehr sind solche Entscheidungen grundsätzlich von Menschen zu treffen. 329

Als **Beispiel** für automatisierte Entscheidungen nennt **EG 71 Satz 1 DSGVO** die **automatische Ablehnung eines Online-Kreditanspruchs oder Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen**. Nach neuerer Rechtsprechung des **Europäischen Gerichtshofs**²⁵² ist **automatisiert erstelltes Scoring** zur Beurteilung der Wahrscheinlichkeit der Erfüllung zukünftiger Zahlungsverpflichtungen als Grundlage für die Entscheidung über den Vertragsschluss als automatisierte Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO zu bewerten. **Vergleichbare von einem KI-System generierte Inhalte dürften regelmäßig als automatisierte Entscheidung in diesem Sinne** einzustufen sein, vorausgesetzt sie entfalten selbst rechtliche Wirkung oder wirken zumindest faktisch determinierend. Generell werden dabei **sowohl tatsächliches Handeln als auch – belastende und begünstigende – Verwaltungsakte** erfasst. 330

Das grundsätzliche Verbot automatisierter Letztentscheidung gilt gemäß **Art. 22 Abs. 2 DSGVO** nur in den drei dort aufgeführten ausdrücklichen **Ausnahmefällen** nicht: 331

- Die Entscheidung ist für den **Abschluss oder die Erfüllung eines Vertrags** zwischen der betroffenen Person und dem Verantwortlichen unbedingt erforderlich (**Art. 22 Abs. 2 Buchst. a DSGVO**).

²⁵⁰ Siehe oben Rn. 208 ff. zum Grundsatz der Datenrichtigkeit.

²⁵¹ Zum Verhältnis von Art. 22 DSGVO und Art. 6 Abs. 3 UAbs. 3 KI-Verordnung Steenbergen, Datenschutzrechtliche Entscheidungsfindung als Hochrisiko-KI-Systeme, KIR 2025, 326.

²⁵² Urteil vom 7. Dezember 2023, C-634/21 „SCHUFA“. Als ausschlaggebend wurde angesehen, dass das „Handeln des Dritten, dem der Wahrscheinlichkeitswert übermittelt wird, maßgeblich von diesem Wert geleitet wird“ (Rn. 48).

V. Datenschutz-Grundverordnung

- Die automatisierte Entscheidung ist aufgrund einer **unions- oder nationalrechtlichen Rechtsvorschrift** zulässig und diese enthält **angemessene Maßnahmen** zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person (**Art. 22 Abs. 2 Buchst. b DSGVO**).

Hinweise: Die Rechtsvorschriften in diesem Sinne müssen die durch Art. 22 Abs. 2 Buchst. b, Abs. 4 DSGVO geforderten **angemessenen Sicherungsinstrumente** selbst festlegen. Insoweit stellen Rechtsvorschriften, die lediglich einen Ausschluss von Ermessen und Beurteilungsspielraum regeln und keine weiteren Garantien vorsehen (wie beispielsweise § 35a Verwaltungsverfahrensgesetz), für sich genommen keine taugliche Rechtsgrundlage in diesem Sinne dar. Ausreichend dürfte dagegen § 6g Abs. 2 Straßenverkehrsgesetz in Verbindung mit §§ 15b, 15f Fahrzeug-Zulassungsverordnung sein, der nur antragsgemäße begünstigende Entscheidungen zulässt, die zusätzlich unter Vorbehalt einer Nachprüfung stehen.

Zu den notwendigen Schutzmaßnahmen können nach EG 71 Abs. 1 Satz 4 ff. DSGVO **insbesondere** gehören:

- Recht der betroffenen Person, das direkte Eingreifen einer Person (das heißt eines Amtsträgers der verantwortlichen Stelle) zu erwirken;
- Recht auf Darlegung des eigenen Standpunkts;
- Recht auf Anfechtung beziehungsweise „Rüge“ der Entscheidung, insbesondere dann, wenn im konkreten Verfahren kein Widerspruch statthaft ist;
- Recht der betroffenen Person auf spezifische Unterrichtung nach Art. 13 Abs. 2 Buchst. f DSGVO und Art. 14 Abs. 2 Buchst. g DSGVO (hierzu gleich Rn. 337);
- Recht auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung;
- Sicherstellung, dass im Regelfall keine Kinder betroffen sind;
- technische und organisatorische Maßnahmen zur Gewährleistung einer fairen und transparenten Verarbeitung, insbesondere um das Risiko von Fehlern zu minimieren und diskriminierende Wirkungen zu vermeiden.

Die Schutzmaßnahmen müssen so gewählt werden, dass sie die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Personen wahren und insoweit „angemessen“ im Sinne von Art. 22 DSGVO sind. Die unionsrechtliche oder nationale Regelung muss also durch entsprechende Vorgaben sicherstellen, dass eine automatisierte Entscheidung den Anforderungen an ein faires und transparentes Verfahren genügt. Für Datenverarbeitungen durch ein KI-System bedeutet dies – bereits aufgrund ihrer Eingriffsintensität –, dass mindestens die vorgenannten Schutzmaßnahmen (kumulativ) vorzusehen sind. Bei Verarbeitungen besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO sind die nochmals erhöhten Anforderungen aus Art. 22 Abs. 4, Art. 9 Abs. 2 Buchst. a oder g DSGVO zu berücksichtigen.

- Die betroffene Person hat ihre **ausdrückliche Einwilligung** erteilt (**Art. 22 Abs. 2 Buchst. c DSGVO**).

332 Die Verarbeitung von **besonderen Kategorien personenbezogener Daten** ist ausweislich **Art. 22 Abs. 4 DSGVO** von den Ausnahmefällen nur umfasst, soweit **Art. 9 Abs. 2 Buchst. a oder g DSGVO** gilt und **angemessene Maßnahmen** zum Schutz der Rechte und Freiheiten

3. Datenschutzrechtliche Anforderungen

sowie der berechtigten Interessen der betroffenen Person getroffen wurden (vgl. EG 71 Satz 7 DSGVO).

Auch in diesen Ausnahmefällen muss die betroffene Person darüber **informiert** werden, dass eine vollautomatisierte Entscheidung über sie getroffen wird, inklusive der zugrundeliegenden Logik und der angestrebten Auswirkungen der Entscheidung (hierzu gleich Rn. 337 f.). Die betroffene Person hat – außer es liegt eine gesetzliche Grundlage vor – nach **Art. 22 Abs. 3 DSGVO** zudem das Recht, die Entscheidung anzufechten und ihren Standpunkt darzulegen sowie eine menschliche Intervention zur Überprüfung der Entscheidung zu verlangen.

333

Außerhalb der genannten Ausnahmefälle ist die Zuhilfenahme von KI-Systemen bei Entscheidungsprozessen öffentlicher Stellen damit aber keineswegs ausgeschlossen. Sie ist allerdings an **drei Bedingungen** geknüpft: Damit eine betroffene Person nicht ausschließlich einer automatisierten Entscheidung unterworfen wird, ist es **zwingend notwendig**, dass

334

- die **die Einzelentscheidung treffende Person das Letztentscheidungsrecht** im Sinne eines **tatsächlichen Entscheidungsspielraums** behält,
- bei der Entscheidung neben den Ausgaben des KI-Systems zusätzlich **weitere Faktoren berücksichtigt** werden und
- die von dem KI-System generierten **Ausgaben zwingend auf inhaltliche Richtigkeit und Vollständigkeit überprüft** werden.

Das heißt, es darf nicht maßgeblich auf der Grundlage des Vorschlags eines KI-Systems entschieden werden und muss sich – auch bei nur entscheidungsvorbereitendem Einsatz eines KI-Systems – das Problem von Ankereffekten oder „automation bias“ vergegenwärtigt werden; eine **lediglich formelle Beteiligung eines Menschen** im Entscheidungsprozess ist **nicht ausreichend**.²⁵³ So dürfen insbesondere unzureichende Personalressourcen, Zeitdruck und fehlende Transparenz über den Entscheidungsweg einer KI-Vorarbeit nicht dazu führen, dass Ergebnisse ungeprüft übernommen werden.

335

Beispiel: Eine städtische Wohngeldstelle setzt zur Bewertung von Wohngeldanträgen ein KI-System ein, das diese Anträge auswertet und ein Bewertungsergebnis (Zustimmung/Ablehnung) vorschlägt. Der zuständige Sachbearbeiter übernimmt das Ergebnis und veranlasst den entsprechenden Bescheid.

Erschöpft sich die Übernahme des vorgeschlagenen Ergebnisses nur in der routinemäßigen Bestätigung des zuständigen Sachbearbeiters, ist der Einsatz des KI-Systems in dem Fall vom Verbot des Art. 22 Abs. 1 DSGVO umfasst. Die Letztentscheidung durch den Menschen soll sich nicht in einer symbolischen Geste erschöpfen.²⁵⁴

²⁵³ Zum Ganzen Europäischer Datenschutzbeauftragter, TechDispatch #2/2025 – Human Oversight of Automated Decision-Making, 23. September 2025, Internet: https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-09-23-techdispatch-22025-human-oversight-automated-making_en.

²⁵⁴ Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP 251 rev.01, Stand 2/2018, S. 22, Internet: <https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html>.

V. Datenschutz-Grundverordnung

Bei eigenständiger Bewertung unter Berücksichtigung der Hinweise des KI-Systems handelt es sich dagegen regelmäßig um eine autonome menschliche Entscheidung.

- 336 Die Einhaltung dieser Erfordernisse ist durch entsprechende **Ausgestaltung des Entscheidungsprozesses**, inklusive einer transparenten **Dokumentation** des Entscheidungswegs, sicherzustellen.²⁵⁵
- 337 Zusätzlich ist darauf zu achten, dass die betroffene Person gemäß **Art. 13 Abs. 2 Buchst. f, Art. 14 Abs. 2 Buchst. g DSGVO** in Ausformung des Transparenzgrundsatzes des Art. 5 Abs. 1 Buchst. a DSGVO **über das Bestehen einer automatisierten Entscheidungsfindung sowie mit aussagekräftigen Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen** einer derartigen Verarbeitung zu informieren ist. Die **Intransparenz und oftmals mangelnde Nachvollziehbarkeit von komplexen KI-Systemen erschwert diese Information in der Praxis häufig**. Hinzu kommt, dass die Informationen für die betroffenen Personen gemäß Art. 12 Abs. 1 DSGVO, **EG 58 Satz 1 DSGVO** in präziser, leicht zugänglicher und verständlicher Form sowie in klarer und einfacher Sprache abgefasst sein müssen.
- 338 Konkret zum **mit diesen Informationspflichten eine Einheit bildenden Auskunftsrecht nach Art. 15 Abs. 1 Buchst. h in Verbindung mit Art. 22 DSGVO** hat der Europäische Gerichtshof entschieden, dass die Vorgabe, das Bestehen einer automatisierten Entscheidungsfindung einschließlich der Logik, Tragweite und angestrebten Auswirkungen zu beauskunften, in der **Praxis** bedeutet, dass der Verantwortliche der betroffenen Person **anhand der maßgeblichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form die Verfahren und Grundsätze erläutern muss, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses konkret angewandt** wurden.²⁵⁶ Dabei genügen weder die bloße Übermittlung einer komplexen mathematischen Formel (etwa eines Algorithmus, dessen Preisgabe im Übrigen auch nicht erforderlich ist) noch die detaillierte Beschreibung jedes Schritts einer automatisierten Entscheidungsfindung diesen Anforderungen, da beides keine ausreichend präzise und verständliche Erläuterung darstellt.²⁵⁷ Durch diese Weiterentwicklung des

²⁵⁵ DSK, Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen (Fn. 121), S. 16.

²⁵⁶ EuGH, Urteil vom 27. Februar 2025, C-203/22 (Dun & Bradstreet Austria) unter Bezugnahme auf EG 71 KI-Verordnung. Die Entscheidung über die Reichweite der Auskunftspflichten in Abwägung zur Geheimhaltungsbedürftigkeit schutzwürdiger Daten von Dritten oder von Betriebs- oder Geschäftsgeheimnissen trifft dabei die zuständige Aufsichtsbehörde oder das zuständige Gericht, vgl. EG 63 Sätze 5 und 6 KI-Verordnung. Nach Auffassung des Europäischen Datenschutzbeauftragten sollte dies auch für automatisierte Entscheidungsvorbereitungen gelten, Europäischer Datenschutzbeauftragter, Generative AI and the EUDPR. Orientations for ensuring data protection compliance when using Generative AI systems (Version 2), 28. Oktober 2025, S. 28, Internet: https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf.

²⁵⁷ Hierzu OLG Stuttgart, Hinweisbeschluss vom 3. Februar 2026, 9 U 148/25, LS 3 und 4: „3. Der Auskunftsan-spruch nach Art. 15 Abs. 1 lit. h DSGVO ist erfüllt, wenn die verantwortliche Stelle die einbezogenen Datenkategorien, die grundlegende Prognoselogik, die Bildung statistischer Vergleichsgruppen sowie Zweck und Tragweite des Scorewerts nachvollziehbar erläutert. Maßgeblich ist, dass die betroffene Person die Richtigkeit ihrer Daten und die Rechtmäßigkeit der Verarbeitung überprüfen kann. Eine weitergehende technische Detailoffenlegung ist hierfür nicht erforderlich. 4. Die Mitteilung der konkreten Gewichtung einzelner Bewertungsfaktoren

3. Datenschutzrechtliche Anforderungen

Auskunftsanspruchs zu einem „Recht auf Erläuterung“²⁵⁸ soll der Vorgabe des Art. 22 Abs. 1 DSGVO Rechnung getragen werden, die eine entsprechende Kenntnis der betroffenen Person erfordert (Auskunftsrecht als „Schlüsselrecht“). Praktisch bedeutet dies, dass die Verantwortlichen **im Hinblick auf die Erfüllung des Anspruchs aus Art. 15 Abs. 1 Buchst. h DSGVO bereits bei den nach Art. 13 und Art. 14 DSGVO bereitzustellenden Informationen entsprechende Transparenz** herstellen müssen, wobei eine **normspezifische Auslegung** vorzunehmen ist.²⁵⁹

Dem nachzukommen, kann für Verantwortliche insbesondere dann herausfordernd sein, wenn sogar Experten die eingesetzten KI-Systeme und die mit diesen einhergehenden Datenverarbeitungsprozesse aufgrund ihrer Komplexität und Architektur nicht mehr eindeutig nachvollziehen können (sogenannte „**Black Box**“, im Gegensatz zu sogenannten „White Box-Modellen“²⁶⁰). Als Lösungsvorschlag hierfür wird in Forschung und Praxis das Konzept der sogenannten „**Explainable Artificial Intelligence (XAI)**“ (deutsch: erklärbare Künstliche Intelligenz) diskutiert: XAI in diesem Sinne umfasst Modelle und Techniken, die entweder selbsterklärend (intrinsisch erklärbar)²⁶¹ sind, „by Design“²⁶² oder im Nachhinein („post hoc“)²⁶³ ein Black Box-Modell erklären können oder eine Kombination dieser Ansätze, ist allerdings mit einigen Limitationen und Problemen verbunden.²⁶⁴ (Derzeit) praktikabler scheint die Überlegung, dass unter Berücksichtigung der Zielsetzung der Art. 13 Abs. 2 Buchst. f,

339

ist nicht geschuldet, da sie faktisch der Offenlegung der Berechnungsformel gleichkäme. Art. 15 Abs. 1 lit. h DSGVO verlangt Transparenz über Verfahren und maßgebliche Kriterien, nicht jedoch die Preisgabe des Algorithmus. Besteht zudem ein nachvollziehbarer Zusammenhang zwischen negativen Zahlungseinträgen und einer schlechteren Bewertung, entsteht kein weitergehendes Aufklärungsbedürfnis.“ Eine Verpflichtung der Offenlegung der Gewichtung dagegen bejahend OLG Dresden, Urteil vom 7. Oktober 2025, 4 U 884/24, und VG Wiesbaden, Urteil vom 19. November 2025, 6 K 788/20.WI.

²⁵⁸ ABhoff, EuGH zum Recht auf Erklärbarkeit bei automatisierten Entscheidungen nach Art. 22 DSGVO, Datenschutz-Berater 2025, S. 245, 246.

²⁵⁹ Siehe auch Bortnikov, Transparenz bei KI-Systemen, DuD 2025, S. 297, 298 f. So müssen die Informationen nach Art. 13 und Art. 14 DSGVO bereits vor Beginn der Datenverarbeitung bereitgestellt werden und können daher nur die allgemeine Funktionsweise und keine Erklärung des Zustandekommens konkreter Ergebnisse der Datenverarbeitung umfassen. Das Auskunftsrecht des Art. 15 Abs. 1 Buchst. h DSGVO betrifft dagegen eine bereits erfolgte oder gegenwärtig erfolgende Datenverarbeitung und damit auch deren konkretes Ergebnis.

²⁶⁰ Diese Modelle bieten sofortige Einblicke in den Entscheidungsprozess, sind selbsterklärend und benötigen daher keine spezifische Post-hoc-Erklärbarkeit. In der Regel sind solche Modelle allerdings eher klein.

²⁶¹ So bieten beispielsweise Algorithmen wie Entscheidungsbäume oder lineare Regressionsmodelle eine hohe Interpretierbarkeit.

²⁶² Goncalves/Correia, Engineering Explainable AI Systems for GDPR-Aligned Decision Transparency: A Modular Framework for Continuous Compliance, Journal of Cybersecurity and Privacy 2026, 6, 7, Internet: <https://www.mdpi.com/2624-800X/6/1/7>.

²⁶³ Geforscht wird dabei zu vier grundlegenden Ansätzen zur Gewinnung von Post Hoc-Erklärungen: verhaltensbasiert, attributionsbasiert, konzeptbasiert und mechanistisch, Cordier/Ditz/Heck/Lazar/Müller, Einfache Darstellung von Komplexität, DuD 2025, S. 250, 252 f. Beispielhaft zu nennen sind LIME (Local Interpretable Model-agnostic Explanations) zur approximativen Darstellung der Entscheidungslogik, SHAP (Shapley Additive exPlanations) zur Quantifizierung des Einflusses jedes Eingabemerkmals auf das Ergebnis oder Counterfactual Explanations zur Eingrenzung der ausschlaggebenden Parameter für eine Entscheidung.

²⁶⁴ Zum Ganzen Bundesamt für Sicherheit in der Informationstechnik, Whitepaper „Erklärbarkeit von KI im adversarialen Kontext“, Stand 11/2024, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Whitepaper_Erklaerbarkeit_KI.html.

V. Datenschutz-Grundverordnung

Art. 14 Abs. 2 Buchst. g, Art. 15 Abs. 1 Buchst. h DSGVO, Transparenz bei der Verwendung von algorithmenbasierten Datenverarbeitungssystemen zu schaffen, und der Vorgaben der Art. 12 Abs. 1 DSGVO und EG 58 DSGVO, den betroffenen Personen eine verständliche und nachvollziehbare Information zur Verfügung zu stellen, sowie unter Berücksichtigung der Rechtsprechung²⁶⁵ **aus dem Transparenzgrundsatz nicht zwingend gefolgert werden muss, dass die betroffenen Personen die genaue Funktionsweise des jeweiligen KI-Systems nachvollziehen können** müssen.²⁶⁶ Derartige Systeme sind regelmäßig so komplex, dass eine Offenlegung etwa des Quellcodes für die durchschnittliche betroffene Person letztlich ohne echten Erkenntnisgewinn und Mehrwert wäre. Vielmehr sollte es in einer den Besonderheiten von KI-Systemen angemessenen Rechnung tragenden Auslegung und Anwendung des Transparenzgrundsatzes **genügen, Funktionsweise und Ausrichtung des jeweiligen Systems abstrakt zu beschreiben**, indem die **Lern-, Arbeits- und (Weiter-) Entwicklungsprozesse** im Rahmen des rechtlich und technisch Möglichen unter Berücksichtigung der verarbeiteten Daten umfassend dargestellt werden und damit sowohl hinsichtlich des **konkreten Ergebnisses als auch hinsichtlich der konkreten Prozesse und dem Zustandekommen einer Entscheidung ein möglichst hohes Transparenzniveau** erreicht wird²⁶⁷. Unterstützend kann hier die auf der Grundlage der KI-Verordnung zu erstellende technische Dokumentation herangezogen werden.

340 **Hinweis:** Die Wirkweise einer Künstlichen Intelligenz kann beispielsweise auch **grafisch** mit Visualisierungen wie Entscheidungsbäumen oder Gewichtsdarstellungen, mit zielgerichteten **Beispielen** oder anhand eines **Musterprozesses** dargestellt werden, mit dem Ziel, ein Grundverständnis der eingesetzten Technik und der mit dieser einhergehenden (Dimension der) Datenverarbeitungsvorgänge zu erreichen.

²⁶⁵ Insbesondere EuGH, Urteil vom 27. Februar 2025, C-203/22.

²⁶⁶ Busche, Potenzial und Grenzen eines Einsatzes von Large Language Models in der öffentlichen Verwaltung, JZ 2024, S. 1007, 1013: „Allerdings gibt es auch keine rechtliche Anforderung einer umfassenden Techniktransparenz; vielmehr entspricht es dem seit langem akzeptierten Normalfall, dass im hoheitlichen Bereich Entscheidungen getroffen werden, ohne dass deren Entstehung im Detail vollständig nachvollzogen werden kann. Auch menschliche Amtswalter sind prinzipiell als Black Box anzusehen. Es kommt darauf an, dass das Verhalten nicht in jedem Detail erklärt, sondern im Wesentlichen nachvollzogen und kontrolliert werden kann.“ Fresz/Dubovitskaya/Brajovic/Huber/Horz, How Should AI Decisions Be Explained? Requirements for Explanations from the Perspective of European Law, Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (2024), 7(1), S. 438, 442 f.: „Each user should be shown the most complex explanation this user can still grasp, requiring an adaption of the explanation to the context“.

²⁶⁷ Generalanwalt Pikamäe, Schlussanträge vom 16. März 2023 in der Rechtssache C-634/21 (SCHUFA), Rn. 58: „Aus den dargelegten Gründen bin ich 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 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.“; DSK, Hambacher Erklärung (Fn. 107), S. 3; Busche, Potenzial und Grenzen eines Einsatzes von Large Language Models in der öffentlichen Verwaltung, JZ 2024, S. 1007, 1013, zieht einen Vergleich zu einer Begründung im Sinne des § 39 Verwaltungsverfahrensgesetz.

3. Datenschutzrechtliche Anforderungen

Im Fall einer automatisierten Entscheidungsfindung ist zudem eine **Datenschutz-Folgenabschätzung** durchzuführen²⁶⁸ (hierzu unten Rn. 349 ff.). 341

Zum Verhältnis von Art. 22 DSGVO und den zugehörigen Informationspflichten zum Recht der betroffenen Personen auf Erläuterung der Entscheidungsfindung im Einzelfall nach **Art. 86 KI-Verordnung** siehe oben Rn. 45. 342

dd) Technische und organisatorische Datenschutzaspekte

Nach **Art. 24 DSGVO** haben verantwortliche Stellen im Hinblick auf die jeweilige Verarbeitung und unter Berücksichtigung der mit ihr einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen zu treffen, wirksam umzusetzen und nachzuweisen**. Diese Verpflichtung wird insbesondere durch die Vorgaben des **Art. 25 DSGVO** („Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“) und des **Art. 32 DSGVO** („Sicherheit der Verarbeitung“) **näher konkretisiert**. Art. 24 Abs. 1 Satz 1 und Art. 32 Abs. 1 DSGVO legen jeweils fest, dass die Geeignetheit von technischen und organisatorischen Maßnahmen unter Berücksichtigung der Risiken für die Rechte und Freiheiten natürlicher Personen geprüft werden muss. Aus Art. 32 Abs. 1 und 2 DSGVO ergibt sich, dass die **Geeignetheit solcher technischer und organisatorischer Maßnahmen in zwei Schritten zu beurteilen** ist: Zum einen sind die **von der Verarbeitung ausgehenden Risiken für die Rechte und Freiheiten natürlicher Personen** zu ermitteln. Diese Beurteilung muss konkret unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der ermittelten Risiken erfolgen. Zum anderen ist zu prüfen, ob die von der verantwortlichen Stelle getroffenen **Maßnahmen** unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke dieser Verarbeitung **diesen Risiken angemessen** sind.²⁶⁹ Neben dem Verantwortlichen hat auch ein Auftragsverarbeiter die Sicherheit der Verarbeitung nach Maßgabe des Art. 32 DSGVO zu gewährleisten. 343

KI-Systeme sind dabei als **IT-Systeme** einzustufen, die regelmäßig als **technische Betriebsmittel** eingesetzt werden und bayerische öffentliche Stellen so bei der Aufgabenerledigung unterstützen sollen. Verarbeitet ein solches KI-System personenbezogene Daten, sind daher vor dem Einsatz nach Ermittlung der Risiken geeignete technische und organisatorische Maßnahmen zu implementieren.²⁷⁰ 344

²⁶⁸ Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 rev.01, Stand 10/2017, S. 10, Internet: <https://www.datenschutz-bayern.de/dsfa/>.

²⁶⁹ EuGH, Urteil vom 14. Dezember 2023, C-340/21, Rn. 83.

²⁷⁰ Einen Überblick gibt Glerean, Fundamentals of Secure AI Systems with Personal Data, EDSA Support Pool of Experts Programme, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/fundamentals-secure-ai-systems-personal_en.

V. Datenschutz-Grundverordnung

345 Neben den **allgemeinen Risiken** bei der Verarbeitung von personenbezogenen Daten mit technischen Systemen sind dabei **für KI-Systeme insbesondere auch folgende Risikobereiche** zu prüfen:²⁷¹

- Ausgabe von unrichtigen oder erfundenen personenbezogenen Daten („**Halluzinationen**“) oder von unerwünschten Daten aufgrund von Desinformation und Verzerrung („**Model Misalignment**“) oder Verlust von Mehrdeutigkeiten („Ambiguity Collapse“)²⁷²;
- Manipulation der Trainingsdaten („**Data Poisoning**“);
- Manipulation durch Eingabedaten, beispielsweise zu Missbrauchszwecken („**Prompt Injection**“, „**Jailbreak**“);
- Überlastung durch umfangreiche Eingaben („**Denial of Service**“);
- **Fehlverhalten** von KI-Systemen.²⁷³

346 Abhängig von den festgestellten Risiken, dem konkreten Einsatzszenario und der Art des KI-Systems können **unterschiedliche Maßnahmen geeignet und umzusetzen** sein.

347 In Betracht kommen **insbesondere**:²⁷⁴

- Etablierung eines restriktiven Rechte- und Rollenkonzepts, insbesondere auch für das Training;
- Festlegung der Prozesse zur Bearbeitung der Anträge auf Geltendmachung der Betroffenenrechte nach Art. 15 ff. DSGVO;
- Festlegung der Speicherdauer; Löschkonzept, insbesondere unter Berücksichtigung der in KI-Systemen verwendeten spezifischen Speicherstrukturen und Zugriffsmechanismen (aufgrund der Nutzung komplexer und verteilter Speichersysteme einschließlich Cloud-basierter Dienste gegebenenfalls Erschwerung der Lokalisierung und Löschung von Daten über verschiedene Standorte und Rechtsordnungen hinweg); der Einsatz von abgeschotteten Systemen ist vorzugswürdig;

²⁷¹ Siehe Europäischer Datenschutzbeauftragter, Guidance for Risk Management of Artificial Intelligence Systems, Stand 11/2025, Internet: https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-11-11-guidance-risk-management-artificial-intelligence-systems_en. Vgl. hierzu auch den derzeit noch in Abstimmung befindlichen Entwurf der ISO/IEC DIS 27090 zum Umgang mit Sicherheitsbedrohungen und Kompromittierungen von KI-Systemen, Internet: <https://www.iso.org/standard/56581.html>.

²⁷² Vgl. Fn. 154.

²⁷³ Versuche unter Testbedingungen haben gezeigt, dass viele der untersuchten Modelle bei drohender Abschaltung oder Situationen, bei denen die Ausrichtung eines Unternehmens nicht mehr zu den vorgegebenen Zielen der Modelle passte, zu Erpressung (teils mit privaten Informationen), Geheimnisverrat an Konkurrenten oder Industriespionage neigten. Anweisungen per Systemprompt konnten die Wahrscheinlichkeit des Fehlverhaltens nur reduzieren. Zum Ganzen iX 8/2025, S. 12.

²⁷⁴ Siehe auch Europäischer Datenschutzbeauftragter, Guidance for Risk Management of Artificial Intelligence Systems (Fn. 271) sowie Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, KI in Behörden – Datenschutz von Anfang an mitdenken, Handreichung der BfDI für die Bundesverwaltung, Stand 12/2025, S. 42 ff., Internet: <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2025/Handreichung-KI.html?nn=251944>.

3. Datenschutzrechtliche Anforderungen

- Qualifizierung von Administratoren;
- regelmäßige Kontrollen des KI-Systems;
- Notfallkonzept (inklusive Backup-Konzept für das KI-System);
- Dokumentation der Trainingsdaten und deren Quellen;
- datenschutzkonforme Protokollierung der Nutzung und des Verhaltens des KI-Systems sowie Auswertung;
- im Verhältnis zu eigenen Beschäftigten eine Dienstanweisung oder Dienstvereinbarung (siehe Rn. 374 ff.), insbesondere zu folgenden Aspekten:
 - Festlegung sogenannter „Use-Cases“ und Prozesse, bei denen eine KI-Nutzung erlaubt ist, einschließlich konkreter Vorgaben, auf welche Art und Weise ein KI-System bei der Erledigung von Arbeitsaufgaben eingesetzt werden darf; Festlegung untersagter Nutzungen;
 - Vermittlung von Risiken und prinzipiellen Einschränkungen von KI-Systemen;
 - Schulungen und Informationen für Beschäftigte;
 - grundsätzliches Verbot der Eingabe personenbezogener Daten; bei (beschränkter) Erlaubnis der Eingabe personenbezogener Daten gegebenenfalls besondere Regeln und Maßnahmen für sensible Daten, wie solche nach Art. 9 Abs. 1, Art. 10 DSGVO oder beispielsweise Geschäftsgeheimnisse;
 - Kontrolle der Ausgaben/Ergebnisse eines KI-Systems auf ihre Richtigkeit, Personenbeziehbarkeit und Diskriminierungsfreiheit;
 - grundsätzliches Verbot von automatisierten Entscheidungen im Einzelfall durch KI-Systeme (mit Blick auf Art. 22 DSGVO);
 - ausdrückliche Aufforderung zur Einhaltung der Datenschutzbestimmungen und anderer rechtlicher Vorgaben;
- Bereitstellung dienstlicher Geräte und Accounts einschließlich Vorgaben zur gegebenenfalls erforderlichen Erstellung/Nutzung dienstlicher, wenn möglich nicht personalisierter Nutzerkonten;
- sichere Authentifizierungsverfahren (Multi-Faktor-Authentifizierung);
- bei selbst oder spezifisch im Auftrag erstellten KI-Systemen datenschutzkonformes Customizing; bei Nutzung eines „Standardprodukts“ zentrale IT- oder zumindest nutzerseitige Einstellungen und Konfigurationen wie beispielsweise Opt-Out, das heißt Abwahl, bezüglich des Weitertrainings eines KI-Systems mit den Eingabedaten und/oder bezüglich der Speicherung des Eingabeverlaufs („Historie“);

V. Datenschutz-Grundverordnung

- Filter oder sonstige Maßnahmen zur Gewährleistung von Fairness, Nichtdiskriminierung („bias“²⁷⁵) und Anonymität;²⁷⁶
- frühzeitige Beteiligung des behördlichen Datenschutzbeauftragten vor Entwicklung und Einsatz von KI-Systemen sowie im Bedarfsfall kontinuierliche Beteiligung während der Nutzung.

348 Die DSK bietet mit dem **Standard-Datenschutzmodell (SDM)** ein Werkzeug zur Unterstützung der risikoadäquaten Auswahl und rechtlichen Bewertung der von der Datenschutz-Grundverordnung geforderten technischen und organisatorischen Maßnahmen.²⁷⁷ Dieses kann auch bei Entwicklung und Einsatz von KI-Systemen unterstützen.

ee) Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

349 Sowohl die Initiierung von KI-Systemen (Trainingsphase) als auch deren Nutzung in einem bestimmten Kontext sind mit datenschutzrechtlichen Risiken verbunden, wenn das KI-System in diesen Phasen personenbezogene Daten verarbeitet.²⁷⁸ Wie bei anderen Verarbeitungen gilt auch hier der Grundsatz, dass **vor der Verarbeitung** die verantwortliche Stelle zu prüfen hat, ob eine Datenschutz-Folgenabschätzung (DSFA) nach **Art. 35 DSGVO** durchgeführt werden muss **oder ein anderer Nachweis zu führen ist** (zum Beispiel eine allgemeine datenschutzrechtliche Risikoanalyse).

350 Art. 35 Abs. 1 Satz 1 DSGVO **erfordert eine DSFA, wenn eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat**, was „insbesondere bei **Verwendung neuer Technologien**“ gilt.²⁷⁹ Für den spezifischen Fall des „Einsatz[es] von KI zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den betroffenen Personen oder zur Bewertung persönlicher Aspekte der

²⁷⁵ Hierzu ausführlich Shrishak, Bias evaluation (Fn. 107), mit Differenzierung der möglichen Maßnahmen in „pre-processing“ (Datenverwaltung, Datenblätter, Kausalanalyse, Umwandlung, Umetikettierung, Neugewichtung, Probenauswahl, Erzeugung künstlicher Trainingsdaten), „in-processing“ (Regulierung, eingeschränkte Optimierung, kontradiktorischer Ansatz, Fine-tuning, Training mit Tags, verstärkendes Lernen mit menschlichem Feedback) und „post-processing“ (Kalibrierung, Schwellenwertregeln) und Auflistung möglicher Werkzeuge. Laurito/Davis/Grieter/Gavenčiak/Böhm/Kulveit, AI-AI bias: Large language models favor communications generated by large language models, PNAS 2025, Vol. 122 No. 31 weisen zudem auf das Risiko hin, dass LLM von Künstlicher Intelligenz generierte Inhalte gegenüber von Menschen generierten Inhalten bevorzugen.

²⁷⁶ Vgl. hierzu Shrishak, Effective implementation of data subjects' rights (Fn. 248).

²⁷⁷ Version 3.1, von der 107. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 14. Mai 2024 beschlossen, Internet: <https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf>. Vgl. auch Halvani/Müller, Sicherheitsanforderungen an KI-Systeme, DuD 2025, S. 302. Vgl. auch DSK, Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0, Stand 6/2025, Internet: https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf.

²⁷⁸ Zur Risikobewertung von KI-Systemen allgemein Europäischer Datenschutzbeauftragter, Guidance for Risk Management of Artificial Intelligence Systems (Fn. 271).

²⁷⁹ Zu Datenschutz-Folgenabschätzungen ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Orientierungshilfe, Stand 2/2021, Internet: <https://www.datenschutz-bayern.de/dsfa/>.

3. Datenschutzrechtliche Anforderungen

betroffenen Personen“ verpflichtet **Nr. 9 Bayerische Blacklist**²⁸⁰ nach Art. 35 Abs. 4 DSGVO zur Durchführung einer DSFA. Aber auch in sonstigen Fällen der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Systemen wird mit Blick auf die **DSFA-Kriterien (insbesondere Nr. 1 „Bewerten oder Einstufen (Scoring)“, Nr. 2 „automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung“, Nr. 5 „Datenverarbeitung in großem Umfang“, Nr. 6 „Abgleichen oder Zusammenführen von Datensätzen“ und Nr. 8 „innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen“)** in Ausfüllung der Vorgaben des Art. 35 Abs. 1, 3 DSGVO regelmäßig eine DSFA vorzunehmen sein.²⁸¹

Hinweis: Bei der Bewertung des Risikos sind auch die **gesetzlichen Kategorisierungen von KI-Systemen nach der KI-Verordnung zu berücksichtigen:** Sind KI-Systeme bereits nach der KI-Verordnung als Hochrisiko-KI anzusehen, liegt nahe, dass ihre Nutzung auch datenschutzrechtlich zu einem hohen Risiko führt. 351

Bei KI-Systemen besteht die Besonderheit, dass nicht selten die verantwortliche Stelle, die ein KI-System für eigene Zwecke nutzt, ein schon trainiertes oder selbst trainierbares KI-System von einer anderen Stelle beschafft und gegebenenfalls von dieser oder einer dritten Stelle betreiben lässt. Dabei fehlt der verantwortlichen Stelle regelmäßig ein vertiefter Einblick in die technischen und organisatorischen Verarbeitungsmodalitäten der anderen Stellen. Diese fehlende vertiefte Kenntnis lässt jedoch die Pflicht der verantwortlichen Stelle unberührt, bei Vorliegen der Voraussetzungen des Art. 35 Abs. 1 Satz 1 DSGVO eine DSFA durchzuführen und nachzuweisen. 352

Hinweis: In der Praxis ist daher eine DSFA, die sich gegebenenfalls aus **mehreren Teilen** zusammensetzt, bei der alle relevanten Stellen ihren Beitrag einfließen lassen und damit gemeinsam für den erforderlichen Mindestumfang der DSFA sorgen, ein tragfähiger Lösungsansatz. 353

²⁸⁰ Bayerischer Landesbeauftragter für den Datenschutz, „Datenschutz-Folgenabschätzung - Bayerische Blacklist - Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO für den bayerischen öffentlichen Bereich“, Stand 1/2019, Internet: <https://www.datenschutz-bayern.de/dsfa/>. Die Bayerische Blacklist orientiert sich an den von der Artikel-29-Datenschutzgruppe veröffentlichten „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt‘“ (Fn. 268), die der Europäische Datenschutzausschuss gebilligt hat. Sie ergänzt und konkretisiert diese Leitlinien sowie Art. 35 Abs. 3 DSGVO.

²⁸¹ Nach den Leitlinien der Artikel-29-Datenschutzgruppe (siehe Fn. 268), S. 10 ff., müssen folgende neun Kriterien (DSFA-Kriterien) berücksichtigt werden, um Verarbeitungsvorgänge zu ermitteln, für die aufgrund ihres hohen Risikos eine Datenschutz-Folgenabschätzung erforderlich ist:

- (1) Bewerten oder Einstufen (Scoring),
- (2) automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung,
- (3) systematische Überwachung,
- (4) vertrauliche oder höchstpersönliche Daten,
- (5) Datenverarbeitung in großem Umfang,
- (6) Abgleichen oder Zusammenführen von Datensätzen,
- (7) Daten zu schutzbedürftigen betroffenen Personen,
- (8) innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen,
- (9) betroffene Personen werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung beziehungsweise Durchführung eines Vertrags gehindert.

V. Datenschutz-Grundverordnung

Dies sollte schon im Vorfeld bedacht und durch entsprechende **(vertragliche) Vereinbarungen** abgesichert werden.

Zumindest sollte der externe Anbieter eines KI-Systems zur Bereitstellung der für die Durchführung einer DSFA erforderlichen Informationen verpflichtet werden.

354 Angesichts der Dynamik der Entwicklungen im Bereich der Künstlichen Intelligenz soll nach der Durchführung einer DSFA zudem **regelmäßig kontrolliert** werden, ob sich die für die DSFA relevanten Umstände womöglich geändert haben und eine Aktualisierung der DSFA erfordern.

355 **Hinweis:** Empfehlungen zu einer aufgeteilten DSFA sowie zu anderen wichtigen Aspekten für die DSFA-Durchführung können einem umfangreichen Informationspaket auf der Website des Bayerischen Landesbeauftragten für den Datenschutz entnommen werden, das in der Praxis für unterschiedliche Verarbeitungskonstellationen erprobt wurde.²⁸²

ff) Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

356 Jede verantwortliche Stelle muss ein Verzeichnis aller Verarbeitungstätigkeiten führen, die ihrer Zuständigkeit unterliegen (**Art. 30 Abs. 1 Satz 1 DSGVO**). Das Verzeichnissesverzeichnis dient in erster Linie dem Nachweis, dass die Verarbeitung personenbezogener Daten durch die verantwortliche Stelle im Einklang mit den datenschutzrechtlichen Vorgaben erfolgt, und soll insbesondere der Datenschutzaufsichtsbehörde ähnlich einer Inventarliste den Einstieg in die Rechtmäßigkeitskontrolle erleichtern.

357 Der Begriff „**Verarbeitungstätigkeit**“ umfasst alle Verarbeitungsvorgänge und Vorgangsreihen, die einem gemeinsamen festgelegten Zweck dienen. Daher bedarf das Verzeichnis von Verarbeitungstätigkeiten abhängig davon, mit welcher Zwecksetzung ein KI-System personenbezogene Daten verarbeitet, einer Ergänzung.²⁸³ Falls beispielsweise eine verantwortliche Stelle ein KI-System trainiert, indem in der KI-Lernphase personenbezogene Daten von dem KI-System verarbeitet werden, ist eine solche Verarbeitung als neue Verarbeitungstätigkeit anzusehen und in das Verzeichnis aufzunehmen. Beim parallelen Training mehrerer KI-Systeme mit unterschiedlichen KI-Technologien, Kategorien personenbezogener Daten und gegebenenfalls Empfängern in einem Drittland empfiehlt es sich, jeweils einen eigenen Eintrag im Verzeichnis aufzunehmen.²⁸⁴

gg) Drittlandübermittlungen (Art. 44 ff. DSGVO)

(1) Allgemein

358 Sowohl im Zusammenhang mit der Nutzung eines KI-Systems als auch bei seiner Entwicklung kann es, je nach tatsächlichen Gegebenheiten, zu **Datenübermittlungen in Länder außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung**, das heißt der

²⁸² Bayerischer Landesbeauftragter für den Datenschutz, Internet: <https://www.datenschutz-bayern.de/dsfa/>.

²⁸³ Bayerischer Landesbeauftragter für den Datenschutz, Frühjahrsputz im Verzeichnissesverzeichnis, Aktuelle Kurz-Information 47, Stand 04/2023, Internet: <https://www.datenschutz-bayern.de/infothek/>.

²⁸⁴ Bayerisches Landesamt für Datenschutzaufsicht, Datenschutzkonforme Künstliche Intelligenz - Checkliste mit Prüfkriterien nach DS-GVO, Stand 1/2024, S. 4, Internet: <https://www.lida.bayern.de/de/ki.html>.

3. Datenschutzrechtliche Anforderungen

Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums (sogenannte Drittländer), kommen.²⁸⁵ **Typischerweise** finden Drittlandübermittlungen bei der Nutzung eines (fremdentwickelten) KI-Systems als **Cloud-Lösung** statt, wenn der Server der Cloud sich in einem Drittland befindet oder unabhängig vom Serverstandort zumindest Meta- und Telemetriedaten in ein Drittland übermittelt werden. Denkbar ist aber auch eine Drittlandübermittlung aufgrund der **Einräumung von Zugriffsrechten** auf ein KI-System (und die darin enthaltenen personenbezogenen Daten) für ein in einem Drittland ansässiges Mutter- beziehungsweise Tochterunternehmen des Anbieters.

Wie in allen Fällen der (möglichen) Übermittlung personenbezogener Daten in Drittländer müssen öffentliche Stellen als datenschutzrechtlich Verantwortliche bereits im Vorfeld des Einsatzes eines KI-Systems sorgfältig prüfen, ob aufgrund des KI-Einsatzes personenbezogene Daten in Drittländer übermittelt werden und ob sich dies gegebenenfalls vermeiden lässt. In Betracht kommt hier insbesondere die eigenverantwortliche Nutzung eines KI-Systems in eigener abgeschlossener IT-Umgebung. 359

Liegt ein Drittstaatentransfer vor, sind die zusätzlichen Anforderungen an die Rechtmäßigkeit der Übermittlung personenbezogener Daten an Drittländer nach **Art. 44 ff. DSGVO** zu beachten.²⁸⁶ Danach ist zunächst zu prüfen, ob ein **gültiger Angemessenheitsbeschluss der Europäischen Kommission** für das Drittland im Sinne von **Art. 45 Abs. 1 und 3 DSGVO** vorliegt.²⁸⁷ Ist dies nicht der Fall beziehungsweise ist ein Angemessenheitsbeschluss auf den betreffenden Sachverhalt nicht anwendbar, so kommt eine **Datenübermittlung vorbehaltlich geeigneter Garantien (vgl. EG 108 DSGVO) sowie durchsetzbarer Rechte und wirksamer Rechtsbehelfe für die betroffenen Personen gemäß Art. 46 Abs. 1 DSGVO** in Betracht, vorausgesetzt diese Garantien gewährleisten ein Schutzniveau für die übermittelten personenbezogenen Daten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist. Die Garantien können gemäß **Art. 46 Abs. 2 Buchst. c DSGVO** insbesondere in sogenannten **Standarddatenschutzklauseln** bestehen. Ein entsprechendes aktuelles Klauselwerk hat die Europäische Kommission im Sommer 2021 bereitgestellt.²⁸⁸ Dieses muss aber – ebenso wie die sonstigen in Art. 46 Abs. 2 DSGVO genannten Garantien – **tatsächlich wirksam** sein, das heißt, die Rechtslage im Drittland muss dem Datenimporteur die Einhaltung seiner vertraglichen Verpflichtungen ermöglichen. Ist dies nicht der Fall, muss 360

²⁸⁵ Zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, KI ohne Grenzen? Einsatz von Drittlandsprodukten in der bayerischen Verwaltung, Aktuelle Kurz-Information 60, Stand 03/2025, Internet: <https://www.datenschutz-bayern.de/infotehk>.

²⁸⁶ Siehe hierzu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Orientierungshilfe, Stand 5/2023, sowie Erste Hilfe zum Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework, Aktuelle Kurz-Information 51, Stand 08/2023, jeweils Internet: <https://www.datenschutz-bayern.de/infotehk/>.

²⁸⁷ Für die Vereinigten Staaten von Amerika (USA), deren Unternehmen den Markt im Bereich Software und IT-Ausstattung weithin dominieren, hat die Europäische Kommission am 10. Juli 2023 einen Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework (deutsch: Datenschutzrahmen EU-USA) erlassen. Damit attestiert sie den USA ein angemessenes Schutzniveau für personenbezogene Daten, die innerhalb dieses Rahmens aus der Europäischen Union an zertifizierte US-Unternehmen als Datenimporteure übermittelt werden.

²⁸⁸ Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. EU L 199 vom 7. Juni 2021, S. 31.

V. Datenschutz-Grundverordnung

der Datenexporteur auf der Grundlage einer **Prüfung der Datenschutzsituation im Drittland**²⁸⁹ zusätzliche Maßnahmen ergreifen, die geeignet sind, die Einhaltung des Schutzniveaus zu gewährleisten. Kann die Übermittlung weder auf einen Angemessenheitsbeschluss nach Art. 45 Abs. 1 DSGVO noch auf geeignete Garantien nach Art. 46 Abs. 1 DSGVO gestützt werden, sieht **Art. 49 DSGVO als Auffangtatbestand** Ausnahmen für bestimmte Fälle von Drittlandübermittlungen vor.

361 Daneben müssen öffentliche Stellen als datenschutzrechtlich Verantwortliche die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 ff. DSGVO gewährleisten und mit Blick auf die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nachweisen. So sind etwa das Erfordernis einer Rechtsgrundlage sowie die umfassenden Informationspflichten nach Art. 13, Art. 14 DSGVO (mit **Spezifika betreffend Drittstaaten-transfers in Art. 13 Abs. 1 Buchst. f, Art. 14 Abs. 1 Buchst. f DSGVO**) (auch) für Datenübermittlungen an Drittländer zu beachten.

362 **Hinweis:** Mit Blick auf die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO ist es öffentlichen Stellen zu empfehlen, grundsätzlich nicht mit Drittlands-Anbietern von KI-Systemen zusammenzuarbeiten, die intransparent im Hinblick auf die von ihnen (im Auftrag) vorgenommene Verarbeitung personenbezogener Daten agieren.

(2) Sonderfall: Cloud

363 **Besonders komplex** stellen sich die Rechtmäßigkeitsvoraussetzungen der datenschutzkonformen **Nutzung von KI-Systemen mittels Cloud** dar, da die im Serververbund **verarbeiteten (personenbezogenen) Daten – jedenfalls** für den für die Verarbeitung dieser Daten Verantwortlichen und damit in der Regel für die öffentliche Stelle als **Betreiber – territorial nicht mehr „einem Server“ und einem bestimmten geografischen Ort zugeordnet** werden können und damit nicht transparent sind und die **Verarbeitung der Daten** in der Regel nicht durch den Betreiber selbst, sondern **durch den Anbieter des cloudbasierten KI-Systems** erfolgt, welcher insoweit **regelmäßig als Auftragsverarbeiter** für den Nutzer als datenschutzrechtlich Verantwortlichen anzusehen ist.²⁹⁰

²⁸⁹ Hierzu ausführlicher Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers (Fn. 286), Rn. 66 ff.

²⁹⁰ Hierzu jeweils m. w. N. ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren (Fn. 103), Rn. 85 ff., sowie Leitfaden zum Outsourcing kommunaler IT, Stand 03/2021, Internet: <https://www.datenschutz-bayern.de/infotehke/>; DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 16. Juni 2025, Confidential Cloud Computing, Internet: BayLfD: https://www.datenschutz-bayern.de/inhalte/dsk_ent_t.htm, und Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023, Kriterien für Souveräne Clouds, Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023, Internet: https://www.datenschutzkonferenz-online.de/weitere_dokumente.html. Speziell zu potentiellen Drittlandzugriffen DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, Beschluss vom 31. Januar 2023, Internet: <https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html>.

3. Datenschutzrechtliche Anforderungen

Diese Besonderheiten führen zu einer Vielzahl von (datenschutz-)rechtlichen Problemen und sind bereits bei der Entscheidung über die Inanspruchnahme der betreffenden Leistung zu berücksichtigen und durch eine entsprechende Vertragsgestaltung möglichst abzusichern. 364

hh) Einbindung der/des behördlichen Datenschutzbeauftragten

Nach **Art. 38 Abs. 1 DSGVO** ist der oder die behördliche Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen und damit auch in Bezug auf KI-Systeme einzubinden. **Art. 12 Abs. 1 Satz 1 Nr. 2 BayDSG** spezifiziert diese Pflicht dahingehend, dass dem oder der behördlichen Datenschutzbeauftragten vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme zu geben ist. Darüber hinaus ist eine kontinuierliche Einbindung der oder des behördlichen Datenschutzbeauftragten im weiteren Verlauf angezeigt. 365

VI. Umsetzungsempfehlungen

- 366 **Grundsätzlich** ist insbesondere die Nutzung von KI-Systemen im Zusammenhang mit und bei der Erfüllung öffentlicher Aufgaben möglich, sofern die gesetzlichen Bestimmungen dies zulassen und alle anwendbaren rechtlichen Anforderungen erfüllt werden, auch in Anbetracht der **besonderen Verantwortung des öffentlichen Sektors, die uneingeschränkte Achtung der Grundrechte und -freiheiten des Einzelnen bei der Nutzung neuer Technologien sicherzustellen**.
- 367 Alle Phasen des Lebenszyklus' eines KI-Systems müssen mithin im Einklang mit den geltenden rechtlichen Rahmenbedingungen stehen und **bei Verarbeitung personenbezogener Daten insbesondere die Vorgaben der Datenschutz-Grundverordnung wahren**.²⁹¹
- 368 Damit einher geht das **Erfordernis der Gewährleistung sogenannter vertrauenswürdiger und verantwortungsvoller Künstlicher Intelligenz**. Dieses Erfordernis bezieht sich auf die Notwendigkeit sicherzustellen, dass KI-Systeme auf ethische²⁹² und rechtmäßige Weise entwickelt und genutzt werden. Hierfür müssen die (auch unbeabsichtigten) Folgen des Einsatzes von KI-Technologie berücksichtigt und muss auch ein risikobasierter Ansatz verfolgt werden, der alle Phasen des Lebenszyklus' der Systeme umfasst. KI-Systeme, die nach diesen Grundsätzen transparent, erklärbar, kohärent, überprüfbar und zugänglich sind, bilden die **Grundlage für eine faire Verarbeitung personenbezogener Daten**.
- 369 In der Praxis sollten insbesondere die folgenden Hinweise berücksichtigt werden:
- **Planung und Beschaffung**
- 370 Die Beschaffung und der Einsatz von KI-Systemen sind unter Berücksichtigung der oben angeführten Vorgaben nicht nur des Datenschutzrechts sondern auch der anderen Rechtsgebiete sorgfältig zu planen und durchzuführen;²⁹³ **aus Effizienz- und Kostengründen** sowie zur Ermöglichung von Synergieeffekten bietet sich gegebenenfalls sogar eine organisationsübergreifende, landesweite strategische Steuerung an.²⁹⁴
- 371 Insbesondere sollte in Anbetracht der regelmäßig großen Datenmengen im Bereich der Künstlichen Intelligenz geprüft werden, ob und inwieweit die Verarbeitung personenbezogener Daten überhaupt erforderlich ist oder deren Umfang durch **Anonymisierung**

²⁹¹ Umfassend Almada, Law & Compliance in AI Security & Data Protection (Fn. 20).

²⁹² Siehe hierzu Gutachten der Datenethikkommission vom 23. Oktober 2019, Internet: <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html>.

²⁹³ Vgl. hierzu allgemein Bayerischer Landesbeauftragter für den Datenschutz, Datenschutzkonzepte für Digitalisierungsvorhaben (Fn. 6).

²⁹⁴ Es ist vorgesehen, am IT-DLZ Bayern eine Stelle einzurichten und aufzubauen, bei welcher Informationen zu KI-Anwendungen bereitgestellt werden sollen.

reduziert werden kann. Mit in den Blick zu nehmen ist dabei auch die **Erforderlichkeit und Sinnhaftigkeit** im Sinne eines echten Mehrwerts **aus Nutzersicht** („Usability“).

– **Technisch-organisatorische Sicherungsmaßnahmen**

Im Zusammenhang mit Gestaltung und Einsatz von KI-Systemen müssen technisch-organisatorische Sicherungsmaßnahmen ergriffen werden (hierzu umfassend oben Rn. 343 ff.), welche insbesondere das Risiko eines Abhandenkommens von oder des unbefugten Zugriffs auf personenbezogene Daten verhindern oder zumindest verringern. 372

– **Erlass einer Experimentierklausel**

Zur Erprobung von KI-Systemen zur Verarbeitung personenbezogener Daten könnte neben der Spezialregelung des Art. 59 KI-Verordnung zusätzlich an den gesetzgeberischen Erlass einer nationalrechtlichen sogenannten „Experimentierklausel“ gedacht werden. Vorstellbar ist beispielsweise eine vorübergehende gesetzliche Ausnahmeregelung, die bei im Labor vortesteten Systemen eine Grundlage für die begrenzte, begleitete und überwachte Nutzung in der Praxis bietet. 373

– **Festlegung interner Regelungen, Erlass einer Dienstanweisung oder Dienstvereinbarung, Beschränkung der zur Nutzung erlaubten Dienste**

Ohne klare Regelungen, ob und wie KI-Systeme im Arbeitsalltag eingesetzt werden dürfen, besteht das Risiko, dass Beschäftigte KI-Systeme eigenmächtig und unkontrolliert nutzen (sogenannte „**Schatten-IT**“). Dies kann zu Datenschutzverstößen führen oder auch zu anderen Schäden für die jeweilige Organisation. 374

Daher sollten, gegebenenfalls unter Benennung eines Ansprechpartners, unter Berücksichtigung sämtlicher rechtlicher Vorgaben klare interne Vorgaben aufgestellt und dokumentiert werden, ob, unter welchen Voraussetzungen und zu welchen konkreten Zwecken welche KI-Systeme eingesetzt werden dürfen und wie mit deren Ergebnissen umzugehen ist. 375

Gegebenenfalls sind konkrete Beispiele der zugelassenen und der untersagten Einsatzszenarien – einschließlich (Un-)Zulässigkeit einer Privatnutzung – zu geben und die erlaubten und gesperrten KI-Systeme beziehungsweise die Interaktionen mit diesen zu benennen und Regelungen zum Umgang mit Verstößen zu treffen. 376

Beispiel: Eine öffentliche Stelle erlaubt allgemein oder nur bestimmten Beschäftigten den Einsatz eines Großen Sprachmodells, verbietet allerdings die Eingabe personenbezogener Daten/von Daten mit besonderem Vertrauensschutz.

Zu diesem Zweck bietet sich neben der **Festlegung interner Regelungen wie Leitlinien für das Datenschutzmanagement und/oder Richtlinien für eine faire Verarbeitung**, die den Beschäftigten bekannt gemacht und diesen jederzeit zugänglich sind, der **Erlass einer Dienstanweisung oder auch der Abschluss einer Dienstvereinbarung** zwischen Dienststellenleitung und Personalrat an. 377

Diese Regelungen sollten **durch technisch-organisatorische Maßnahmen „abgesichert“** werden, beispielsweise durch Vorschaltung eines informierenden oder warnenden 378

VI. Umsetzungsempfehlungen

Hinweises vor jeder Nutzung des betreffenden KI-Systems oder der regelmäßigen Einwilligung in Nutzungsbedingungen.

– Überprüfung

- 379 Zur Gewährleistung der Einhaltung der datenschutzrechtlichen Rechtmäßigkeitsanforderungen an KI-Systeme zählen auch die **Planung und die regelmäßige sowie anlassbezogene Durchführung von (gegebenenfalls externen) Prüfungen zum Datenschutz**, etwa mit Blick auf die Verlässlichkeit, die Transparenz, die Fairness und die IT-Sicherheit, um einen datenschutzkonformen Betrieb einschließlich der funktionalen und IT-Sicherheit des KI-Systems zu gewährleisten. In diesem Zusammenhang empfiehlt sich gleichzeitig die Etablierung eines Verfahrens zur Umsetzung der Ergebnisse.

– Anforderungs- und Änderungsmanagement

- 380 Es wird empfohlen, Richtlinien und Kommunikationsprozesse für das Anforderungs- und Änderungsmanagement festzulegen, um zu gewährleisten, dass neue Versionen oder Änderungs freigaben von KI-Systemen in einem nachvollziehbaren Prozess geplant, umgesetzt und zum Einsatz gebracht werden.

– Vertragsmanagement

- 381 Werden KI-Systeme nicht selbst entwickelt, sondern zum eigenständigen Betrieb oder als Dienstleistung zur Nutzung eingekauft, kommt dem Vertragsmanagement zwischen verantwortlichem Betreiber und Anbieter des KI-Systems besondere Bedeutung zu: Da im Vertragswerk (hinsichtlich des Datenschutzes oftmals eine Auftragsverarbeitungsvereinbarung im Sinne des Art. 28 Abs. 3 DSGVO²⁹⁵) wesentliche datenschutzrechtliche Fragestellungen wie Zuständigkeiten, technische und organisatorische Maßnahmen und sonstige Einzelheiten geregelt werden, muss deren nachweisliche tatsächliche Einhaltung sichergestellt werden.

– Etablierung von Prozessen zur Gewährleistung der Betroffenenrechte sowie zum Umgang mit Datenschutzverstößen

- 382 Zur Sicherstellung der Wahrnehmung der Betroffenenrechte sowie zum Umgang mit Datenschutzverstößen sind öffentliche Stellen als datenschutzrechtlich Verantwortliche aufgerufen, in Bezug auf die von ihnen im Zusammenhang mit KI-Systemen verantworteten Verarbeitungen personenbezogener Daten gleichförmige transparente Prozesse unter Berücksichtigung der Vorgaben der Datenschutz-Grundverordnung zu etablieren, um eine effektive Behandlung zu ermöglichen.

– Sensibilisierung von Beschäftigten

- 383 Beschäftigte sollten generell, aber auch in (vorausschauender) Umsetzung der Verpflichtung aus **Art. 4 KI-Verordnung** durch Schulungen, Leitfäden und Gespräche regelmäßig dahingehend sensibilisiert werden, ob und wie sie KI-Systeme nutzen sollen und dürfen. Ferner sollten die Stärken und Schwächen des eingesetzten KI-Systems sowie die mit

²⁹⁵ Siehe oben Rn. 293.

VI. Umsetzungsempfehlungen

dessen Einsatz verbundenen datenschutzrechtlichen Herausforderungen aufgezeigt werden.

Insbesondere bei Großen Sprachmodellen ist der Prompt entscheidend für das von der Künstlichen Intelligenz ausgegebene Ergebnis. Es empfiehlt sich daher, den Beschäftigten im Rahmen von Schulungen beizubringen, wie Prompts idealerweise aufgebaut und formuliert werden sollen (sogenanntes „**Prompt Engineering**“) und wie mit den Ausgaben von KI-Systemen umzugehen ist. 384

Im Einzelfall ist auch die Festlegung von Kriterien für die **Auswahl von Beschäftigten**, die spezifische KI-Systeme nutzen dürfen, denkbar, welche in einem entsprechenden **Rechte- und Rollenkonzept/Berechtigungskonzept** gespiegelt wird. Dieses sollte die Anforderungen und Besonderheiten von Künstlicher Intelligenz berücksichtigen und die Rollen, Rechte und Pflichten der beteiligten Akteure klar regeln. Insbesondere kann der **Datenzugriff** auf einen bestimmten Personenkreis (beispielsweise Administratoren) **beschränkt** werden, können **Zugriffsbefugnisse** auf der Grundlage einer Bewertung der Vertraulichkeit der Daten erteilt werden und ist die Umsetzung des Konzepts durch eine Zugangskontrolle zu dem betreffenden KI-System wie beispielsweise ein **Authentifizierungssystem** abzusichern. Die danach mit KI-Systemen befassten Beschäftigten sollten ihrer Rolle angemessen auf der Grundlage von spezifizierten Anforderungsprofilen ausgewählt, sensibilisiert und Qualifizierungsplänen folgend geschult werden. 385

– Prüfung weiterer Entwicklungen

Mit Blick auf die rechtlichen Entwicklungen im Bereich der Künstlichen Intelligenz sowie auf fortschreitende technische Lösungen und laufende Updates²⁹⁶ sollte regelmäßig überprüft werden, ob die internen Vorgaben angepasst werden müssen. Hierzu empfiehlt es sich, eine Routine im Rahmen des betrieblichen Datenschutzmanagements (Art. 24 DSGVO) zu etablieren. 386

– Einbindung des behördlichen Datenschutzbeauftragten

Mit Blick auf die Vorgabe des Art. 38 Abs. 1 DSGVO sowie seine Sachnähe empfiehlt sich die kontinuierliche beziehungsweise zumindest anlassbezogene Einbindung des behördlichen Datenschutzbeauftragten sowie gegebenenfalls des Informationssicherheitsbeauftragten. 387

²⁹⁶ Siehe beispielsweise die Nationale Strategie Künstliche Intelligenz der Bundesregierung, Internet; <https://www.ki-strategie-deutschland.de/> und die „Hightech Agenda Bayern“ sowie die „Hightech Agenda Plus“, Internet; https://www.bayern.de/wp-content/uploads/2019/10/hightech_agenda_bayern.pdf und <https://www.bayern.de/bericht-aus-der-kabinettsitzung-vom-14-september-2020/#a-1>.

VII. Zusammenfassung

- 388 **Technische Entwicklungen datenschutzrechtlich zu begleiten, ist eine wichtige Aufgabe der Datenschutzaufsichtsbehörden, um einerseits deren Datenschutzkonformität zu gewährleisten und andererseits deren Potenzial zu fördern.** Die vorliegende Handreichung soll öffentliche Stellen in Bayern beim Einsatz von KI-Systemen unterstützen und dadurch Rechtsverstößen vorbeugen. **Künstliche Intelligenz und KI-Systeme, die personenbezogene Daten verarbeiten,** sind aufgrund ihrer Vielfalt und Komplexität **zwar ein durchaus anspruchsvolles datenschutzrechtliches Thema, unterliegen aber im Grundsatz den inzwischen über Jahre entwickelten und erprobten Mechanismen zur Umsetzung der Vorgaben der Datenschutz-Grundverordnung.** Damit können öffentliche Stellen insoweit auf **bereits vorhandene Erkenntnisse** zurückgreifen. Der mit der KI-Verordnung einhergehende zusätzliche Aufwand kann mit Hilfe von bereits bestehenden Systemen bewältigt werden, die auf einem ganzheitlichen und verknüpften Datenschutzmanagementsystem mit integriertem Risikomanagement aufbauen. Den öffentlichen Stellen bietet sich insoweit auch die Chance, mit gutem Beispiel voranzugehen und eine Vorreiterrolle bei der datenschutzkonformen Implementierung von Künstlicher Intelligenz einzunehmen.
- 389 **Welche weitere Entwicklung die Künstliche Intelligenz nimmt, wird sich zeigen:** Während einer den nächsten „KI-Winter“ prophezeit²⁹⁷ und der andere die Künstliche Intelligenz sogar schon auf dem Rückzug sieht,²⁹⁸ steht die KI-Entwicklung nach Auffassung Dritter nun an einem Punkt, an dem sie nicht mehr aufzuhalten ist,²⁹⁹ und strebt jedenfalls die Europäische Kommission mit ihrem „Aktionsplan für den KI-Kontinent“ danach, auf dem Gebiet der KI weltweit führend zu werden.³⁰⁰ Tatsache ist, dass die vorhandenen KI-Modelle das Internet „leer“ gelesen haben, aber laufend neue Inhalte von guter Qualität benötigen, um sich weiter

²⁹⁷ So der Robotiker Rodney Brooks am 9. Januar 2024: „Es könnte ein weiterer KI-Winter, vielleicht sogar ein echter Tech-Winter, bevorstehen. Und es wird kalt werden.“, Internet: <https://www.nowadais.com/de/rodney-brooks-vorhersage-im-jahr-2024/>.

²⁹⁸ KI-Entwickler Gary Marcus im Juni 2024: „Merken Sie sich das Datum, der große KI-Rückzug hat begonnen.“, Internet: <https://www.sueddeutsche.de/kultur/ki-winter-zweifel-und-realitaet-lux.ALPKerz4grGTyWPjutgPWL>.

²⁹⁹ Internet: <https://www.sueddeutsche.de/kultur/ki-winter-zweifel-und-realitaet-lux.ALPKerz4grGTyWPjutgPWL>.

³⁰⁰ Europäische Kommission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 9. April 2025, COM(2025) 165 final, Internet: <https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan>. Der Aktionsplan sieht hierfür Maßnahmen und Strategien in den fünf Schlüsselbereichen (1) Aufbau einer großen KI-Daten- und Recheninfrastruktur, (2) verbesserter Zugang zu großen und hochwertigen Datenbeständen, (3) Entwicklung von Algorithmen und Förderung der KI-Einführung in strategischen Sektoren, (4) Entfaltung von KI-Kompetenzen und -Talenten und (5) Vereinfachung der Rechtsvorschriften vor. Zu diesem Zweck wurden unter anderem Konsultationen zum Rechtsakt über Cloud- und KI-Entwicklung, zur Strategie „Apply AI“ (<https://digital-strategy.ec.europa.eu/en/policies/apply-ai>) sowie zur Strategie für eine Europäische Datenunion durchgeführt. Einen Überblick über die Herausforderungen einer globalen KI-Compliance gibt Haar, KI-Regulierung weltweit: Viele eigene Wege, iX 12/2025, S. 97.

VII. Zusammenfassung

optimieren zu können.³⁰¹ Rein synthetisch erzeugte Daten werden hier nur begrenzt ausreichen. Der Schutz personenbezogener Daten wird künftig also weiter – und stärker – gefordert sein.

³⁰¹ So warnen Studien vor dem generativem Kollaps von KI-Generatoren, Shumailov et al., AI models collapse when trained on recursively generated data, Nature 631, S. 755; Alemohammad et al., Self-Consuming Generative Models Go MAD, arXiv:2307.01850, Internet: <https://arxiv.org/abs/2307.01850>; Gerstgrasser et al., Is Model Collapse Inevitable? Breaking the Curse of Recursion by Accumulating Real and Synthetic Data, arXiv:2404.01413, Internet: <https://arxiv.org/abs/2404.01413>.