Datenschutz bei Künstlicher Intelligenz

KARL
Künstliche Intelligenz
für Arbeit und Lernen

Kompetenzzentren
Arbeitsforschung

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

– Autor*innen

Dr. Manuela Bao, Aline Vugrincic, Ann-Katrin Dreher, Daniel Vonderau, Hoa Tran, Maria Rill, Silvia Balaban

FZI Forschungszentrum Informatik, Haid- und Neu-Straße 10-14, 76131 Karlsruhe,
{manuela.bao, vugrincic, dreher, vonderau, tran, m.rill, balaban}@fzi.de, Webseite: www.fzi.de

– Veröffentlichung: 25. August 2023

Inhalt

— 1. Teil: Grundbausteine

1 Einleitung

Der schillernde Begriff der „Künstlichen Intelligenz“ konnte bisher keiner allgemeingültigen Definition zugeführt werden.[1] Zunächst einmal fällt bereits die Frage nach der Definition von „Intelligenz“ schwer.[2] KI wird sodann als Technik bezeichnet, die Maschinen „intelligent“ oder menschenähnlich handeln lässt, um bisher nur von Menschen lösbare Probleme zu bewältigen.[3] Versuche einer rechtlichen Annäherung an eine Definition sind: „Systeme mit einem ‚intelligenten‘ Verhalten, die ihre Umgebung *analysieren* und mit einem gewissen Grad an *Autonomie* handeln, um bestimmte Ziele zu erreichen“[4] oder das Verständnis von KI als technisches System, das Probleme *eigenständig* bearbeiten und sich dabei selbst auf *veränderte* Bedingungen einstellen kann, wobei ihm die Eigenschaft zukommt, aus neuen Daten zu „*lernen*“.[5]

Ein wesentlicher Grund für die schwierige Begriffsverortung der „Künstlichen Intelligenz“ liegt auch in der Bandbreite der Technologien, Einsatzkontexten und -parameter. Allerdings ist eines vielen Anwendungen gemein, welche als „KI-Systeme“ verstanden werden, dass Daten – und dabei mitunter große Datenmengen – erkenntnisstiftend ausgewertet werden.[6] Anhand von Beispielen (Trainingsdaten) werden Modelle trainiert, welches anschließend auf neue, unbekannte Daten angewendet werden kann.[7] Mit diesen „intelligenten“ Modellen bestehend aus tiefen Netzen künstlicher Neuronen, die auf den Trainingsdaten optimiert wurden, können ohne im Vorhinein sämtliche Regeln oder Berechnungsvorschriften manuell festlegen zu müssen Vorhersagen, Empfehlungen oder Entscheidungen generiert werden – als selbstständige Anwendung oder Teil eines Systems.[8] Werden diese Anwendungen und Systeme im Beschäftigungskontext eingesetzt, bieten sich sowohl Chancen als auch Risiken: die Chance für eine effizientere, menschengerechtere und nachhaltigere Gestaltung der Arbeitsorganisation einerseits, aber auch das Risiko einer intensiveren Kontrolle und Überwachung der Beschäftigten.[9] Werden im Zusammenhang mit dem Einsatz eines KI-Systems personenbezogene Daten verarbeitet, bietet das Datenschutzrecht einige Schutzmechanismen um den Persönlichkeitsschutz und die Selbstbestimmung der Beschäftigten zu gewährleisten.

Mit Blick auf die neuen Herausforderungen dieser Technologie lassen sich als wesensimmanente Merkmale die eigenständige Verhaltensweise zur eigenständigen Entscheidungsfindung, die Prognosefähigkeit und die Fähigkeit zu autonomen Lern- und Adaptionsprozessen charakterisieren.[10] Unterschieden wird dabei oftmals zwischen „starker“ und „schwacher“ KI: schwache KI hat die Fähigkeit zur Mustererkennung und kann damit

[1] Siehe zu Definitionsversuchen im rechtswissenschaftlichen Kontext: *Schürmann*, ZD 2022, 316; *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. I 1.; *Ory/Sorge*, NJW 2019, 710 (710 f.).
[2] *Conrad*, DuD 2017, 740 (740); *Schefzig*, DSRITB 2018, 491 (492).
[3] *Ory/Sorge*, NJW 2019, 710 (710); *DFKI/Bitkom e.V.*, Künstliche Intelligenz, S. 14.
[4] *EU-Kommission,* Mitteilung zum Koordinierten Plan für künstliche Intelligenz, COM(2018) 795 final vom 7.12.2018, S. 1.
[5] BT-Drs. 19/1982, S. 2 f. (Antwort auf eine kleine Anfrage zu konkreten Zielen und Vorhaben der Bundesregierung im Bereich künstliche Intelligenz).
[6] Vgl. BT-Drs. 19/1982, S. 2; *EU-Kommission,* Mitteilung zum Koordinierten Plan für künstliche Intelligenz, COM(2018) 795 final vom 7.12.2018, S. 1; *Ory/Sorge*, NJW 2019, 710 (710); *Conrad*, DuD 2017, 740 (740); *Schefzig*, DSRITB 2018, 491 (493); *Wischmeyer*, AöR 2018, 1 (10 ff.); *Niemann/Kevekordes*, CR 2020, 17 (17).
[7] *Fraunhofer IAIS*, Vertrauenswürdiger Einsatz von Künstlicher Intelligenz, S. 10.
[8] *Fraunhofer IAIS*, Vertrauenswürdiger Einsatz von Künstlicher Intelligenz, S. 10.
[9] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 4.
[10] Schürmann, ZD 2022, 316 (316); Schefzig, DSRITB 2018, 491 (492).

auf unbekannte Probleme reagieren ohne dabei außerhalb ihres Kontextes agieren zu können.[11] Sie dienen dazu Menschen „intelligent“ beim Erreichen bestimmter Ziele zu unterstützen.[12] Hierzu zählen auf Machine Learning basierende Anwendungen, wie bspw. Sprachassistenten oder Navigationssysteme.[13] Erst bei „starker“ KI kommt die dem Menschen ebenbürtige intellektuelle Fähigkeit hinzu logisches Denkvermögen zu entwickeln und dabei über die vordefinierte Anwendung hinaus zu agieren – Fähigkeiten, die allerdings noch nicht erreicht wurden.[14] Eine wesentliche Unterscheidung für die rechtliche Betrachtung liegt in reinen Recommender- oder Assistenzsystemen, die einem Menschen lediglich eine Entscheidung vorbereiten, und „algorithmischen Entscheidungssystemen“ im Sinne von Delegationstechnik bei dem die handlungsleitende Letztentscheidung bereits durch die Maschine erfolgt.[15]

Dieses Gutachten behandelt die Grundbausteine des Datenschutzrechts mit besonderem Fokus auf den Beschäftigtendatenschutz, welches eine erste rechtliche Einhegung einer auf der Auswertung personenbezogener Daten basierenden „Künstlichen Intelligenz“ bietet. Darüber hinaus wird derzeit auf EU-Ebene eine KI-spezifische Regulierung erarbeitet,[16] welche in ihren Grundzügen ebenfalls betrachtet wird, um Parallelen und Unterschiede in der Herangehensweise aufzuzeigen. Für ein grundlegendes Verständnis des Datenschutzkonzepts werden zunächst das Rollenmodell und die wesentlichsten Definitionen vorgestellt (Abschnitt 2). Abschnitt 3 behandelt mit den grundrechtlichen Schutzverbürgungen den Hintergrund der datenschutzrechtlichen Regulierung intelligenter Systeme. Rechtliche Vorgaben sind allerdings nur zu befolgen, wenn der jeweilige Anwendungsbereich eröffnet ist (Abschnitt 4). In Abschnitt 5 werden systematisiert nach den Grundprinzipien der Datenschutz-Grundverordnung (DSGVO) die Schutzkonzepte vorgestellt. Einen weiteren Schwerpunkt bilden in Abschnitt 6 die Rechtsgrundlagen, da aufgrund des Verbots mit Erlaubnisvorbehalts jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage bedarf. Besonderheiten gelten in Bezug auf automatisierte Einzelfallentscheidungen, die vergleichend zur geplanten KI-Verordnung in Abschnitt 7 erörtert werden. Im zweiten Teil zu Arbeit und Lernen widmet sich Abschnitt 8 sodann dem Beschäftigtendatenschutz. Ausnahmen im Forschungskontext werden in Abschnitt 9 vorgestellt. Weitere kontextspezifische Datenschutzanforderungen betreffen die strengeren Regeln bezüglich der als besonders sensibel einzustufenden „besonderen Kategorien personenbezogener Daten“, das Recht auf Datenübertragbarkeit, der Datentransfer in Drittländer sowie die elektronische Kommunikation (Abschnitt 10).

In einem weiteren Teil sollen sodann in der zweiten Version dieses Handlungsleitfadens fallspezifische Szenarien des Einsatzes von KI für Arbeit und Lernen in den Anwendungsdomänen Mobilität, Produktion, Wissensarbeit und Bildung vorgestellt werden.

[11] *Fraunhofer-Allianz Big Data*, Zukunftsmarkt Künstliche Intelligenz - Potenziale und Anwendungen, S. 5; *Conrad*, DuD 2017, 740 (740); *Schürmann*, ZD 2022, 316 (316). Andere kategorisieren in: Schwache, starke KI und Superintelligenz: Gausling, DSRITB 2018, 519 (521 m.w.N.).

[12] *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. I 1.

[13] *Schürmann*, ZD 2022, 316 (316); *Gausling*, DSRITB 2018, 519 (521).

[14] *Conrad*, DuD 2017, 740 (740); *Schürmann*, ZD 2022, 316 (316); *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. I 1.; *Gausling*, DSRITB 2018, 519 (521).

[15] Vgl. *Schröter*, Magazin erwachsenenbildung.at. 2022, 15.

[16] *EU-Kommission,* 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 21.4.2021 – COM(2021) 206 final.

2 Rollenmodell und Definitionen im Datenschutzrecht

Für ein fundiertes Verständnis datenschutzrechtlicher Implikationen im Kontext algorithmischer Steuerungs- und Entscheidungssysteme bedarf es zunächst der Definition von Schlüsselbegriffen.

2.1 Definierte Rollen

Die wesentlichen Schutz- und Handlungssubjekte sind in Abbildung 1 skizziert. Die zentralen Rollen sind die der betroffenen Person und des Verantwortlichen. In dessen Sphäre agiert, gewissermaßen als verlängerter Arm, der Auftragsverarbeiter. Weitere Rollen sind die des Empfängers personenbezogener Daten und des Dritten, der weder zu den betroffenen Personen, Verantwortlichen noch Auftragsverarbeitern zählt.

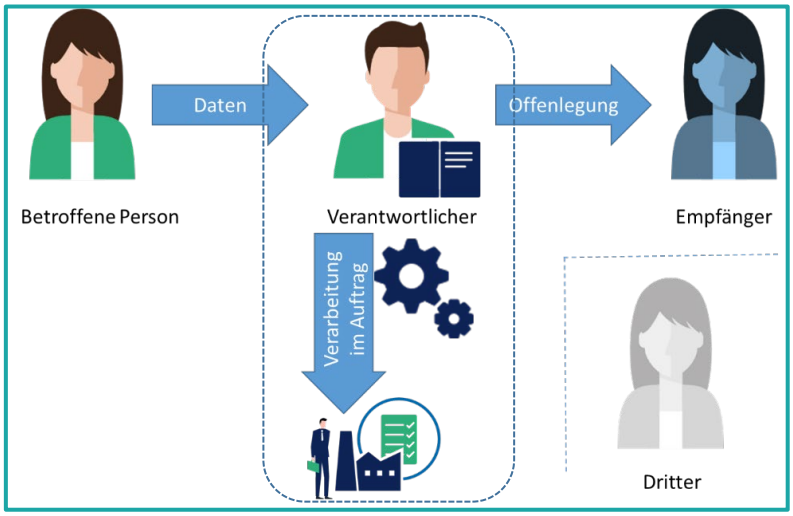


Abbildung 1 Rollenmodell im Datenschutzrecht

2.1.1 Betroffene Person

Zentrales Schutzsubjekt des Datenschutzrechts ist die betroffene Person. Sie wird in Art. 4 Nr. 1 DSGVO legaldefiniert als identifizierte oder identifizierbare natürliche Person. Juristische Personen werden von der DSGVO ausdrücklich nicht erfasst.[17] Gemäß ErwGr. 27 findet die DSGVO keine Anwendung bei der Verarbeitung personenbezogener Daten Verstorbener. Andere Regelungen zum Persönlichkeitsschutz bieten hingegen auch postmortalen Schutz.[18]

[17] *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 5.
[18] Beispiele bei: *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 4.

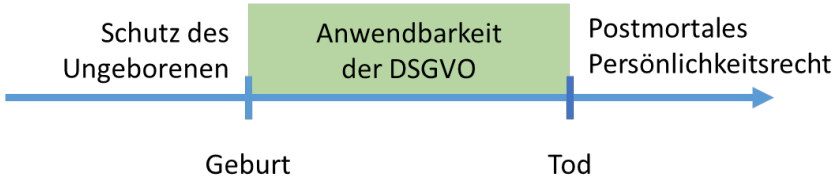


Abbildung 2 Phasen des Persönlichkeitsschutzes

2.1.2 Verantwortlicher

Die Frage nach der Verantwortlichkeit ist eine der zentralen Fragen für die Bestimmung des datenschutzrechtlichen Pflichtenkanons.[19] Die Zuordnung der Verantwortung zu einer bestimmten Stelle entscheidet mit über die territoriale Anwendbarkeit des Datenschutzregimes in internationalen Kontexten. Sie definiert die Adressat*innen der datenschutzrechtlichen Pflichten. Aus Sicht der betroffenen Personen muss bekannt sein, gegenüber welcher Stelle sie ihre jeweiligen Rechte geltend machen können.[20] Auch ist diese Haftungsadressat*in und unterliegt bei Verstößen gegen die datenschutzrechtlichen Pflichten dem Haftungsregime insbesondere den Sanktionsmöglichkeiten der DSGVO.

2.1.2.1 Kriterien zur Bestimmung des Verantwortlichen nach der DSGVO

Der Adressat der datenschutzrechtlichen Vorgaben ist zunächst der sog. „Verantwortliche“ für die Datenverarbeitung, welcher in Art. 4 Nr. 7 DSGVO definiert wird. Danach ergeben sich zwei Weichenstellungen für die Zuordnung der Verantwortlichkeit:

- Entscheidung über Zweck und Mittel der Verarbeitung personenbezogener Daten oder
- Zuweisung durch Unionsrecht oder Recht der Mitgliedstaaten.

> **Art. 4 Nr. 7 DSGVO „Verantwortlicher“**
>
> 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;
>
> sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Entscheidend ist dabei, wer die tatsächliche Entscheidungsbefugnis über die Datenverarbeitung hat[21] sowie über Mittel und Zwecke tatsächlich Entscheidungen treffen kann.[22] Dabei hat der EuGH mehrfach betont, dass durch eine weite Definition des Begriffs des Verantwortlichen ein wirksamer und umfassender Schutz

[19] Der Begriff „Verantwortlicher“ entstammt der deutschsprachigen Version der DSGVO und wird daher nicht gegendert. Vor Inkrafttreten der DSGVO war der Begriff „verantwortliche Stelle“ gebräuchlich, welcher hier synonym weiter genutzt wird.
[20] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 3; *Jung/Hansch*, ZD 2019, 143 (143).
[21] *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 87a.
[22] *Hartung,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 7 Rn. 13.

der betroffenen Personen gewährleistet werden soll.[23]

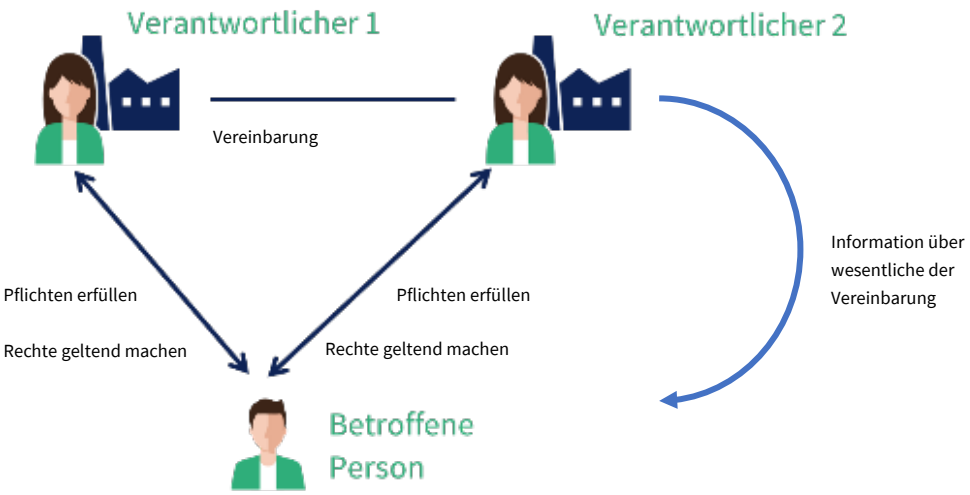
Zweck: Unter „Zweck“ wird das „erwartete Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet“, verstanden.[24] D.h. der Verantwortliche ist diejenige Stelle, welche die Frage beeinflusst, *warum* personenbezogene Daten verarbeitet werden. Abgrenzend zur Auftragsverarbeitung kommt es darauf an, ob Daten zu eigenen Zwecken oder im Auftrag eines Anderen verarbeitet werden bzw. ob aus einem Eigeninteresse heraus Einfluss auf die Verarbeitung genommen wird.[25] Bei mehreren Verantwortlichen liegt eine Entscheidung über den Zweck vor, wenn ein gemeinsames Ziel zum wechselseitigen Vorteil verfolgt wird.[26]

Mittel: Das Mittel beschreibt die Art und Weise, wie ein Ergebnis oder Ziel erreicht wird.[27] Insofern bestimmt der Verantwortliche auch das *Wie* der Verarbeitung.[28] Hier stellen sich oft schwierige Abgrenzungsfragen, welches Level an Einfluss der Verantwortliche haben muss, wenn bspw. die technische Umsetzung stark in der Hand eines Auftragsverarbeiters liegt, der aber keine eigenen Zwecke mit der Datenverarbeitung verfolgt. Wesentliche Aspekte könnten bspw. Entscheidungen über die Auswahl der verarbeiteten Daten, die Einrichtung von Zugangsmöglichkeiten oder die Dauer der Verarbeitung sein.[29]

Angesichts der vom EuGH präferierten weiten Auslegung kann es ausreichen, dass ein Beitrag im Sinne einer Mitwirkung zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten geleistet wird.[30] Wenn eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DSGVO vorliegt, muss nicht einmal ein tatsächlicher Zugang jedes Verantwortlichen zu den Daten bestehen.[31] Ebenso kann es unerheblich sein, wenn sich Stellen formal nicht als Verantwortliche oder Auftragsverarbeiter bezeichnen, da es andernfalls den Parteien eines Vertrages überlassen wäre, über die Wahl der Vertragsbedingungen und Begrifflichkeiten Verantwortung nach eigenen Interessen unabhängig von tatsächlich ausgeübten Entscheidungsfunktionen zuzuweisen.[32]

[23] EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 65; EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 66; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 28; EuGH, Urteil vom 13.05.2014 – C-131/12 – Google Spain, Rn. 34.
[24] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 13.
[25] Vgl. EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 68.
[26] *Schwartmann*, Ordnung der Wissenschaft 2020, 77 (78).
[27] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 13.
[28] *Jung/Hansch*, ZD 2019, 143 (144).
[29] *Niemann/Kevekordes*, CR 2020, 179 (183).
[30] EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 31.
[31] EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 69; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 38; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 69. Zur Kritik siehe: *Niemann/Kevekordes*, CR 2020, 179 (183).
[32] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 12.

2.1.2.2 Die gemeinsame Verantwortung

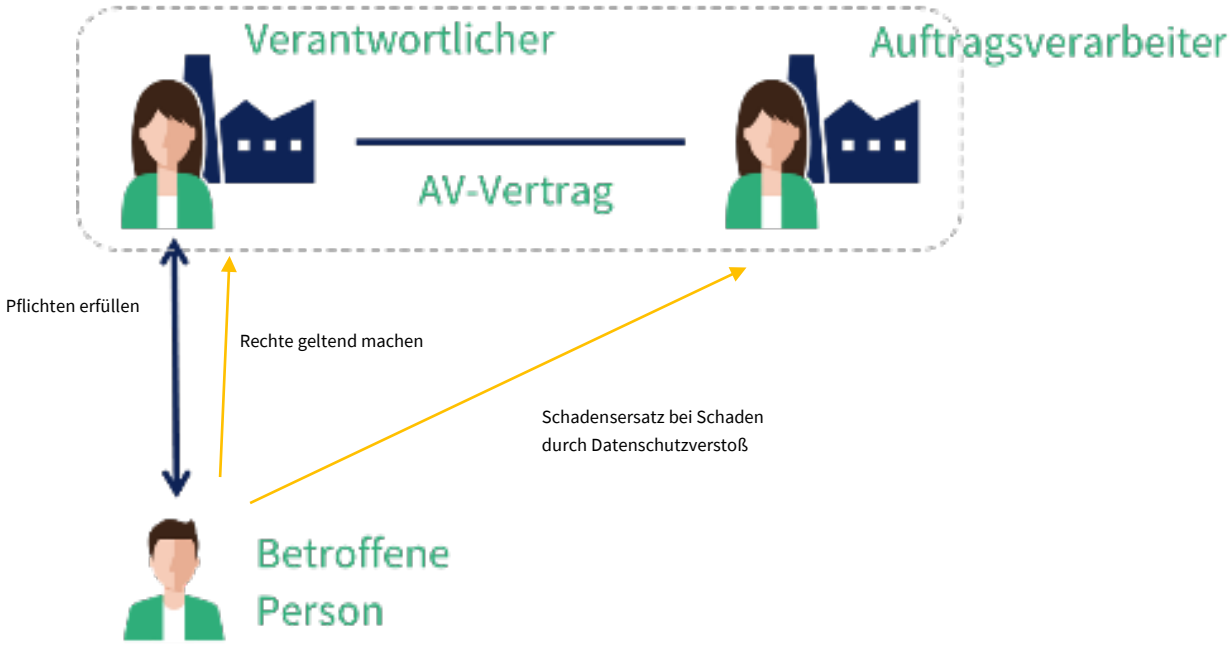


Sofern mehrere Verantwortliche gemeinsam für die Zwecke und Mittel der Datenverarbeitung verantwortlich sind, spricht man von einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO. Wenn also verschiedene Stellen zusammen Verarbeitungsprozesse steuern oder darüber entscheiden, liegt eine solche gemeinsame Verantwortlichkeit vor.[33] Dabei muss nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure gegeben sein.[34] Die unterschiedlichen Stellen können vielmehr in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.[35] Gemeinsam Verantwortliche können dabei zusammen Zweck und Mittel festlegen, oder konvergierend in dem Sinne entscheiden, dass die jeweils getroffene Wahl einander ergänzt und für die Verarbeitung in einer Weise erforderlich ist, sodass sie einen spürbaren Einfluss auf die Festlegung der Zwecke und Mittel der Verarbeitung hat.[36] Ist eine Verarbeitung ohne die Mitwirkung beider Parteien nicht möglich, d.h. dass die Parteibeiträge unauflösbar miteinander verbunden sind, so kann eine konvergierende Entscheidung vorliegen. Dabei gilt jedoch zu berücksichtigen, dass bezüglich Entscheidungen über Zweck und Mittel, die in einer Verarbeitungskette vorausgehen oder nachfolgen, auch Wechsel zwischen alleiniger und gemeinsamer Verantwortlichkeit gegeben sein können.[37]

Liegt eine gemeinsame Verantwortung vor, kann eine Stelle folglich auch dann ein für die Verarbeitung Verantwortlicher sein, den alle Pflichten der einschlägigen DSGVO-Vorschriften treffen, wenn sie nicht *alle* Entscheidungen über die Zwecke und Mittel trifft.[38] Das Verhältnis gemeinsam für die Verarbeitung Verantwortlicher wird durch Art. 26 DSGVO geregelt.

[33] *Hartung,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 7 Rn. 12.
[34] *Forgó,* in: Autonomes Fahren, Kap. 3.5 Rn. 24.
[35] EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 43; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 70.
[36] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 18.
[37] EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 74.
[38] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 13.

2.1.3 Auftragsverarbeiter



Gemäß Art. 4 Nr. 8 DSGVO kann eine natürliche oder juristische Person, eine Behörde, Einrichtung oder andere Stelle auch als Auftragsverarbeiter Daten im Auftrag des Verantwortlichen verarbeiten. Wesentliches Unterscheidungskriterium zu der gemeinsamen Verantwortlichkeit ist die Weisungsgebundenheit des Auftragsverarbeiters, der nur in einem vorgegebenen Rahmen des Auftragsgebers tätig werden darf.[39] Des Weiteren unterliegt der Auftragsverarbeiter nach Art. 28 Abs. 3 DSGVO einer Reihe weiterer Pflichten gegenüber dem Auftraggeber, damit dieser sicher stellen und v.a. kontrollieren kann, dass sein jeweiliger Auftragsverarbeiter die personenbezogenen Daten auch nur im Rahmen des Auftragsdatenverarbeitungsvertrages verarbeitet und sich versichern kann, dass die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters gewährleistet werden können.[40]

Wiederum abzugrenzen von der Auftragsverarbeitung ist der Fall, in dem ein Soft-/Hardware-Hersteller keine Verarbeitung personenbezogener Daten vornimmt, sondern lediglich Soft- bzw. Hardware liefert. Den Lieferanten treffen direkt keine Pflichten der DSGVO, allerdings wird darüber diskutiert inwiefern indirekt über das Gewährleistungsrecht die Datenschutzpflichten des Verantwortlichen gewissermaßen Vorwirkungen entfalten.[41] Einerseits kann das Vorhandensein datenschutzrelevanter Funktionen explizit vertraglich vereinbart sein, sodass ein Produktmangel bei gänzlichem Fehlen oder Fehlfunktionen vorliegt. Andererseits kann sich nach Auslegung der Vertragsbeziehung auch ohne explizite Nennung der Produktmangel aus der fehlenden Eignung zur vorgesehenen Verwendung ergeben, wenn das Produkt zur Verarbeitung personenbezogener Daten im Geltungsbereich des EU-Datenschutzrechts vorgesehen ist.

[39] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 24 f.
[40] Siehe hierzu Abschnitt 2.5.2.2.
[41] *Baumgartner/Gausling*, ZD 2017, 308 (311); *Schuster/Hunzinger*, CR 2017, 141 (146); *Dümeland*, K&R 2019, 22 (24).

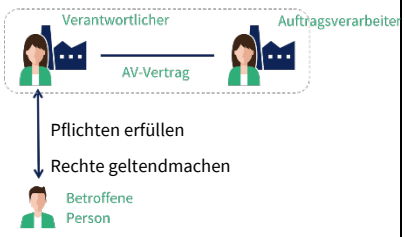
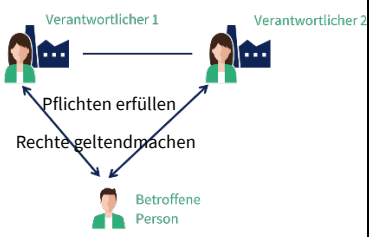
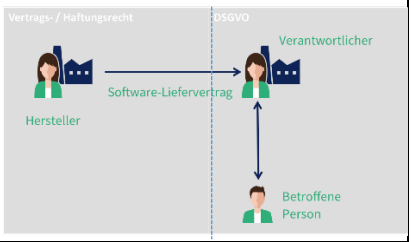
Einzelverantwortung und Auftragsverarbeitung	Gemeinsame Verantwortung	Soft-/Hardware-Hersteller ohne datenschutzrechtliche Verantwortung
		
– Wird als „verlängerter Arm“ des Verantwortlichen tätig – Abschluss AV-Vertrag – Unterstützungspflichten Auftragnehmer – Kontroll- und Weisungsrechte des Auftraggebers – Auftragnehmer darf keine eigenen Verarbeitungszwecke verfolgen	– Vereinbarung mit umfassender Regelung der Verantwortlichkeiten abschließen & bereitstellen – Jeder Verantwortliche bedarf eigener Rechtsgrundlage für Verarbeitung personenbezogener Daten	– Keine Datenschutzpflicht – Datenschutzrelevante Funktionen ggf. vertraglich vereinbart – Produktmangel bei fehlender Eignung zur vorgesehenen Verwendung

Table 1 Überblick zur Verantwortlichkeitsabgrenzung

2.1.4 Sonstige Rollen & Rollenverständnis

Neben den drei zentralen Rollen der betroffenen Person, des Verantwortlichen und des Auftragsverarbeiters kennt die DSGVO noch weitere Rollen, wie den Empfänger personenbezogener Daten sowie den „Dritten“. Erwähnung finden diese Rollen bspw. wenn der Verantwortliche in Datenschutzerklärungen Angaben zu den Empfängern oder Kategorien von Empfängern machen muss, an die personenbezogene Daten weitergeleitet werden. Die Person des Dritten ist bspw. relevant, wenn es darum geht, welche Kenntnisse dem Verantwortlichen zuzurechnen sind, um eine Person identifizieren zu können (siehe Abschnitt 0).

Art. 4 Nr. 9 DSGVO - „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

Art. 4 Nr. 10 DSGVO „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

Art. 4 Nr. 17 DSGVO „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Art. 27 DSGVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

Art. 4 Nr. 18 DSGVO „Unternehmen“ eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

Art. 4 Nr. 21 DSGVO „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle;

Verantwortlicher kann grundsätzlich sowohl eine Privatperson, ein Unternehmen, eine Behörde oder sonstige Stelle sein. Das „Unternehmen“ wird in der DSGVO explizit definiert, sodass kein Rückgriff auf die zivilrechtliche Begriffsbestimmung in § 14 BGB genommen werden muss. Weniger Klarheit herrscht beim Begriff der „Behörde“. Dieser Begriff wird von der DSGVO zwar verwendet, allerdings nicht definiert. Vorgeschlagen wird, Behörde als „jede Stelle, die eine Verwaltungsaufgabe wahrnimmt“ einzugrenzen.[42] Dies stimmt mit der Bestimmung im deutschen Verwaltungsverfahrensgesetzt (VwVfG) überein. Die Behörde wird hierbei durch ihre Funktion bestimmt.[43]

§ 1 Abs. 4 VwVfG Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

Befindet sich der Verantwortliche oder Auftragsverarbeiter nicht innerhalb der EU, muss nach den Vorgaben des Art. 27 DSGVO ein Vertreter in der EU genannt werden.

2.2 Definition: Daten

2.2.1 Daten – Information – Wissen

Während in der Informationswissenschaft der Begriff der Daten nur eine Entwicklungsstufe in einem kognitiven Entscheidungsprozess repräsentiert, werden Differenzierungen zwischen den Begriffen „Daten“, „Information“ und „Wissen“ im Datenschutzrecht nicht nachvollzogen.[44] Die Begriffe Daten und Information werden vielmehr synonym verwendet und sind grundsätzlich weit zu verstehen.[45] Umfasst sind Informationen in jeglicher Form wie Sprache, Schrift, Zeichen, Bild oder Ton – digital oder analog. [46] Im Hinblick auf algorithmische Steuerungs- und Entscheidungssysteme können sowohl die Trainings-, Validierungs- und Testdaten(-sätze), sonstige Eingabedaten als auch die Ergebnisse, also das neu generierte Wissen, über einen Personenbezug verfügen.

2.2.2 Personenbezogene Daten

Angesichts des bezweckten Schutzes der Grundrechte natürlicher Personen bei der Verarbeitung sie betreffender Daten,[47] stehen in sachlicher Hinsicht personenbezogene Daten im Mittelpunkt, die in Art. 4 Nr. 1

[42] *Schnabel,* in: NK Datenschutzrecht Art. 86 Rn. 20.
[43] *Gola,* in: Gola DS-GVO, Art. 4 Rn. 62.
[44] Ausführlich zur Konkretisierung des Datenbegriffs: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 25 ff.
[45] *Klar/Kühling,* in: Kühling/Buchner - DS-GVO/BDSG Art. 4 Nr. 1 Rn. 8.
[46] *Klar/Kühling,* in: Kühling/Buchner - DS-GVO/BDSG Art. 4 Nr. 1 Rn. 9.
[47] Vgl. ErwGr. 1 und 2; siehe auch: *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 7.

DSGVO definiert sind. Danach sind unter personenbezogenen Daten alle Informationen zu verstehen, die sich auf eine *identifizierte* oder *identifizierbare* natürliche Person beziehen. Somit kann die betroffene Person grundsätzlich nur eine natürliche – und keine juristische Person sein.[48] Geschützt werden grundsätzlich alle Menschen unabhängig von ihrer Staatsbürgerschaft oder Unionsbürgerschaft.[49] Bei Angaben zu einer juristischen Person, reinen Unternehmensdaten und Sachinformationen, die auch nicht mittelbar zur Identifizierung einer natürlichen Person geeignet sind, ist das Datenschutzrecht nicht anwendbar.[50]

Die Definition ist weit zu verstehen.[51] Im beruflichen Kontext gilt zu bedenken, dass Daten, welche sich zunächst primär auf ein Unternehmen beziehen, gleichzeitig einen Bezug zu einer natürlichen Person aufweisen können.[52] Besonders deutlich wird das im Fall einer sog. Einmann-GmbH.[53] Ebenso bei Kaufleuten: soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt, können diese sich ebenfalls auf den grundrechtlich verbürgten Schutz ihrer Daten berufen.[54] Folglich bestehen vor allem in diesen Fällen typischerweise Risiken des Durchschlagens:

- Eine E-Mail-Adresse, Social-Media-Account, Messenger-ID, Telefonnummer oder ähnliches weist zwar keine Person namentlich auf, wird allerdings regelmäßig von der gleichen Mitarbeiter*in verwaltet.[55]
- Aussagen über Kleinbetriebe, Vereine oder ähnliche juristische Personen und Personengesellschaften, die sich auch auf das Verhalten der Eigentümer*innen bzw. Gesellschafter*innen, die Geschäftsführer*innen oder den Vorstand, etc. beziehen,[56]
  - Bspw. wenn der Name der juristischen Person vom Namen der natürlichen Person ableitet ist.[57]
  - Bspw. wenn sich aus dem Gesamtzusammenhang ergibt, dass eine natürliche Person alleinige Gesellschafter*in und Geschäftsführer*in ist.[58]

Als natürliche Person geschützt sind somit sowohl Privatpersonen, als auch Angestellte, Selbstständige und beruflich handelnde Personen – sofern sich die Daten auf eine identifizierbare Person beziehen.[59]

Identifizierbarkeit: Für die Frage, ob ein Datum personenbezogen ist oder nicht, kommt es darauf an, ob eine natürliche Person anhand der Daten bereits identifiziert ist oder identifiziert werden kann. Als Möglichkeit zur Identifizierung nennt Art. 4 Nr. 1 DSGVO insbesondere die Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirt-

[48] *Piltz*, K&R 2016, 557 (557). Zur Reichweite des Grundrechtsschutzes aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, 14 Abs. 1, 19 Abs. 3 GG sowie Art 7, Art. 8 EU-GrCh für juristische Personen siehe: *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 6 ff. m.w.N.
[49] *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 10.
[50] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 4.
[51] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 22.
[52] *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 14; *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 13.
[53] BGH, Urteil vom 17-12-1985 - VI ZR 244/84; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 4; *Arning/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 17.
[54] EuGH, Urteil vom 9. 11. 2010 - C-92, 93/09 - Volker und Markus Schecke und Eifert, Rn. 53; *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 7.
[55] *Arning/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 17; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, S. 27.
[56] *Arning/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 17.
[57] EuGH, Urteil vom 9. 11. 2010 - C-92, 93/09 - Volker und Markus Schecke und Eifert, Rn. 53; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, S. 27.
[58] BGH, Urteil vom 17-12-1985 - VI ZR 244/84.
[59] EuGH, Urteil vom 30. 5. 2013 – C-342/12 – Equipamentos para o Lar S/Autoridade para as Condições de Trabalho [ACT]; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 4.

schaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Hierbei macht die verwendete Begrifflichkeit des „insbesondere“ deutlich, dass es sich um sog. Regelbeispiele handelt und die Aufzählung folglich nicht abschließend ist.[60]

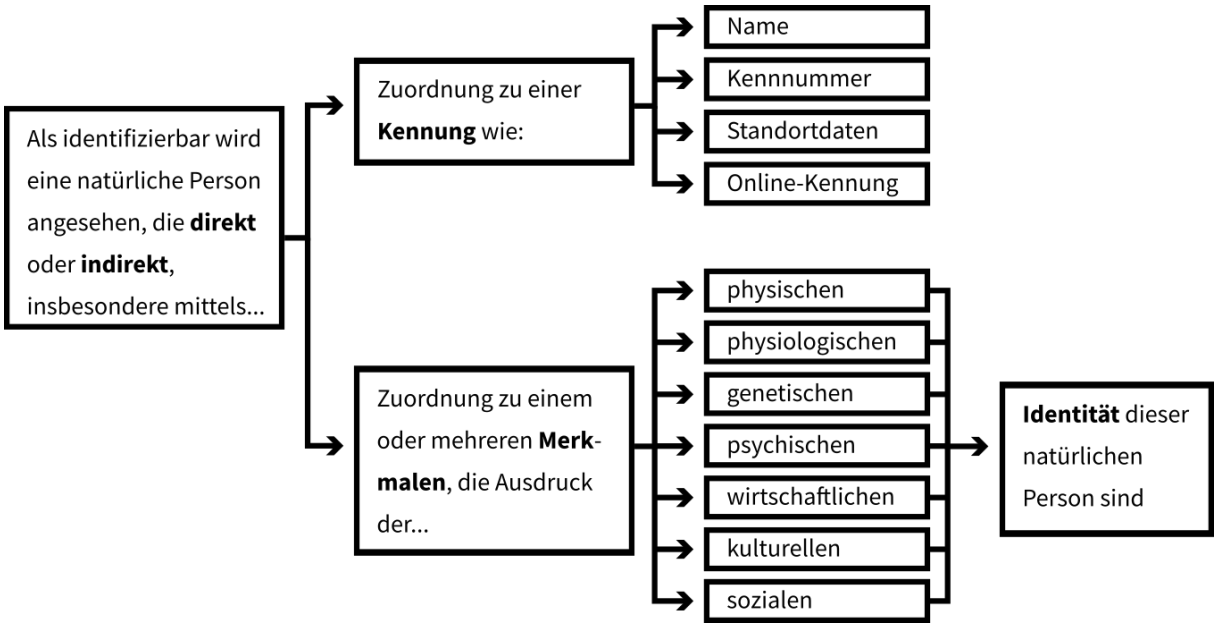


Abbildung 3 Regelbeispiele für die direkte und indirekte Identifizierbarkeit in Art. 4 Nr. 1 DSGVO

Ob eine Person identifizierbar ist, hängt entscheidend von den Informationen ab, zu denen der Verantwortliche Zugang hat. Ein wegweisendes Urteil hat an dieser Stelle der EuGH in der Sache Breyer zur Frage des Personenbezugs dynamischer IP-Adressen gefällt:

EuGH, Urteil vom 19.10.2016 - C-582/14 – Breyer

- Ein personenbezogenes Datum muss nicht für sich genommen die Identifizierung der betreffenden Person ermöglichen.
- Selbst wenn sich die Identität der natürlichen Person nicht unmittelbar aus den vorliegenden Daten ergibt, kann diese identifizierbar sein, wenn entsprechende **Zusatzinformationen** einholbar sind.
- Dies ist nicht der Fall, wenn die Identifizierung der betreffenden Person **gesetzlich verboten** oder **praktisch nicht durchführbar** wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung *de facto* vernachlässigbar erschiene.
- Rechtliche Möglichkeiten sind auch dann gegeben, wenn diese die Mitwirkung eines Dritten, bspw. einer zuständigen Behörde erfordern.

Folglich ist es für die Annahme der Identifizierbarkeit ausreichend, dass grundsätzlich eine Möglichkeit be-

[60] *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 15.

steht, identifizierende Informationen bei einem Dritten einzuholen, selbst wenn hierfür zunächst die Mitwirkung einer Behörde angefragt werden muss.[61] Dieses noch zur Datenschutzrichtlinie ergangene Grundsatzurteil lässt sich auf die DSGVO übertragen.[62] Dies zeigt sich insbesondere in den Erwägungsgründen, die inhaltlich weitgehend auf den bereits zuvor entwickelten Weichenstellungen der Datenschutzrichtlinie beruhen:[63]

ErwGr. 26, S. 3, 4 DSGVO

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Eine Person kann somit bereits dann identifiziert werden, wenn sie sich von allen anderen Personen einer Gruppe eindeutig unterscheiden lässt (Aussondern).[64] Die *Möglichkeit* einer Identifizierung unter verhältnismäßigem Aufwand ist somit ausreichend.[65] Bei KI-Systemen, die Daten automatisch auswerten und neue Datenquellen erschließen, besteht besonders die Gefahr, dass durch Verkettung von Informationen (auch ungewollt) ein Personenbezug hergestellt wird.[66] Sofern Zweifel bestehen, ob personenbezogene Daten vorliegen, können die von der Art-29-Datenschutzgruppe (Vorgänger des Europäischen Datenschutzausschusses - EDSA) noch zur Datenschutzrichtlinie entwickelten Abgrenzungskriterien herangezogen werden:[67]

Die genannten Elemente sind alternativ, nicht kumulativ zu verstehen.[68] Dabei können auch Bezüge zu mehreren Personen bestehen. Bspw. kann eine Aussage inhaltlich auf eine Person bezogen sein und aus den Metadaten[69] Rückschlüsse auf die absendende oder empfangende Person zulassen. Die Erfassung dieser Daten

Artikel-29-Datenschutzgruppe WP 136, 2007

- **Inhaltselement:** Angaben sind eindeutig „über“ eine bestimmte Person
- **Zweckelement:** Daten werden unter Berücksichtigung aller Begleitumstände mit dem Zweck verwendet, eine Person zu beeinflussen, zu beurteilen oder in einer bestimmten Weise zu behandeln
- **Ergebniselement:** die Verwendung könnte sich unter Berücksichtigung aller jeweiligen Begleitumstände auf die Rechte und Interessen einer bestimmten Person auswirken.

[61] EuGH, Urteil vom 19.10.2016 - C-582/14 – Breyer, Rn. 48.
[62] *Klar/Kühling,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 20; *Piltz*, K&R 2016, 557 (561).
[63] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 67 f.
[64] *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (153); *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, S. 14; *Roßnagel*, ZD 2013, 562 (563); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 58 f.
[65] BGH Urteil vom 16. Mai 2017 – VI ZR 135/13; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, S. 14; *Bergt*, ZD 2015, 365 (369); *Kring/Marosi*, K&R 2016, 773; *Jensen/Knoke*, ZD-Aktuell 2016, 05416; *Weinhold*, ZD-Aktuell 2016, 05366; *Kühling/Klar*, ZD 2017, 27; *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 11.
[66] *Schefzig*, DSRITB 2018, 491 (497).
[67] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, S. 7 ff.; bestätigt in der Rechtsprechung des EuGHs zur RL 95/46/EG: EuGH, Urteil vom 20.12.2017 – C-434/16 – Nowak, Rn. 35.
[68] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, S. 13.
[69] Unter Metadaten versteht man Daten, die ihrerseits dazu dienen, ausgewählte Aspekte von (Primär) Daten zu beschreiben, wie z. B. Telefonnummern und sonstige Kontaktdetails, Zeitpunkte bzw. Dauer einer Kommunikation sowie ggf.

kann dem Zweck dienen, diese Personen nachzuverfolgen und/oder kann bestimmte Folgen für diese Personen haben. Beim Ergebniselement werden nicht nur negative oder nachhaltige Folgen erfasst – ausreichend ist, dass „die Person aufgrund der Verarbeitung solcher Daten anders als andere Personen behandelt werden könnte."[70] Damit fallen sowohl persönliche als auch sachliche Angaben unter den Begriff personenbezogene Daten.

- **Persönliche Angaben** sind z.B. Name, Alter, Anschrift, Geschlecht, Geburtsdatum, Telefonnummer, Fingerabdrücke, Fotos oder Videos.[71]
- **Sachliche Angaben** sind etwa die Beziehung des Betroffenen zur Umwelt, Sachen oder Dritten, wie Angaben zum Umfeld, seiner finanziellen Situation, Vertragsbeziehung, Kommunikationsverhalten, etc.[72] Auch die Erfassung von Arbeitszeiten fallen regelmäßig unter die personenbezogene Daten.[73]

Maschinendaten: Im Rahmen der Automatisierung von Arbeitsprozessen werden oftmals Daten aus der Produktion oder Industrieprozessen verwendet. Diese sind auf den ersten Blick als technische Daten über Sachen zu qualifizieren. Insofern wird der Begriff „Maschinendaten" durchaus als Gegensatz zum personenbezogenen Datum genutzt.[74] Allerdings können diese Maschinen Personen direkt zugeordnet sein oder über Zuhilfenahme weiterer Daten zuordenbar. Der Maschineneinsatz, Pausenzeiten und Reparaturzeiten können dann wiederum Rückschlüsse auf das Arbeitsverhalten der die Maschine bedienenden Person liefern. Allein aus dem Begriff „Maschinendaten" sollte daher nicht der Schluss gezogen werden, diese seien nicht-personenbezogen.

Beispiele für personenbezogene Daten:

- (dynamische und statische) IP-Adressen, Cookies, Browser-Fingerprints,
- Telefonnummern,[75] Mail-Adressen, Personalnummer,
- Kfz-Kennzeichen, Adressdaten,
- Zahlungsdaten (Kreditkartennummer, Kontonummer, etc.
- Alter, Geburtsdatum, Familienstand,
- Bild-/Filmmaterial, Gesichts- und Körpermerkmale,
- Genetische Daten, Fingerabdruck, DNA

2.2.3 Besondere Kategorien personenbezogener Daten

Im Rahmen der personenbezogenen Daten genießen besondere Kategorien personenbezogener Daten nach Art. 9 Abs.1 DSGVO höhere Schutzanforderung (sog. sensible Daten). Die Einordnung ist zwar für die Anwendbarkeit der DSGVO nicht von Bedeutung, soll nichtsdestotrotz an dieser Stelle bereits angerissen werden. Zu diesen Daten gehören Angaben über:

- Rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,

Standort der kommunizierenden Parteien, vgl. hierzu: *Krüger/Möllers*, MMR 2016, 728 (728); *Faas*, ArbRAktuell 2018, 594 (595); *Polst u. a.*, DuD 2021, 19 (20).

[70] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 13.

[71] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 14.

[72] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 14.

[73] EuGH, Urteil vom 30. 5. 2013 – C-342/12 – Equipamentos para o Lar S/Autoridade para as Condições de Trabalho [ACT].

[74] Vgl. bspw. *Fries/Scheufen*, MMR 2019, 721.

[75] Auch bei Nebenstellenapparaten, wenn eine Zuordnung zu einzelnen Beschäftigten möglich ist: BAG, Beschluss vom 27.05.1986 - 1 ABR 48/84.

- die Gewerkschaftszugehörigkeit
- genetische Daten,[76] biometrischen Daten[77] zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten[78]
- und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Liegen besondere Kategorien personenbezogener Daten vor, bestehen besonders hohe Anforderungen an die Legitimierung einer Verarbeitung dieser Daten.

Besondere Kategorien personenbezogener Daten in Bilddaten: Oftmals werden Bilddaten verwendet, um bestimmte (Arbeits-)Abläufe, bestimmte Merkmale oder Eigenschaften zu trainieren. So kann bspw. der Baufortschritt auf einer Baustelle mit Bild-/Videomaterial auch remote verfolgt werden. Um Menschen auf diesen Bildern automatisiert zu verpixeln, müssen ebenfalls Personenbilder trainiert werden. Beim autonomen Fahren arbeiten die KI Systeme regelmäßig mit Video-, Lidar- und Radar-Daten.

Grundsätzlich wird bei Bild- und Videodaten der Umstand diskutiert, dass das Äußere teilweise auch Rückschlüsse auf Herkunft (durch Hautfarbe, Augenform, etc.) sowie Gesundheitszustand (bspw. durch körperliche Beeinträchtigungen) ermöglichen kann und das Tragen religiöser Symbole die religiöse oder weltanschauliche Überzeugung anzeigt.[79] Grundsätzlich sollen auch Daten erfasst werden, aus denen die genannten Kategorien mittelbar hervorgehen (bspw. aus dem Gesamtzusammenhang).[80] Dies führte bereits zur Annahme, bei jeglicher Form der Videoüberwachung im öffentlichen Raum seien besondere Kategorien personenbezogener Daten betroffen.[81] Im Rahmen von KI-Systemen werden zumeist Profilbilder genutzt, sodass sich eine ähnliche Problematik stellen würde. Allerdings wurde dieser Einschätzung zu Recht entgegengehalten, dass diskriminierende[82] oder freiheitseinschränkende Wirkungen der Datenverarbeitung erst zu befürchten sind, wenn tatsächlich entsprechende Rückschlüsse gezogen werden, sodass der Schutzzweck der Norm eher die zielgerichtete Erfassung dieser Daten adressiert.[83] Würden bspw. zur Erstellung personalisierter Werbung derartige Informationen abgeleitet, müsste sich diese Tätigkeit nach Art. 9 Abs. 2 DSGVO messen lassen. Das Verbot in Art. 9 Abs. 1 DSGVO ist hingegen nicht eröffnet, wenn diese Daten nur beiläufig er-

[76] Definiert in Art. 4 Nr. 13 DSGVO als: „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

[77] Definiert in Art. 4 Nr. 14 DSGVO als: „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

[78] Definiert in Art. 4 Nr. 15 DSGVO als: „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

[79] Vgl. hierzu *Schneider/Schindler*, ZD 2018, 463 (456 f.).

[80] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 13; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 11.

[81] Schleswig-Holsteinischer Landtag Drucksache 19/429, S. 144.

[82] Hintergrund der Aufnahme der rassischen und ethnischen Herkunft ist u.a. das Diskriminierungsverbot in Art. 21 EU-GrCh, *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 29; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 25; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 15.

[83] Unabhängiges Landeszentrum für Datenschutz (ULD), Schriftliche Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Gesetzentwurf der Landesregierung Drucksache 19/429, S. 8; *Schneider/Schindler*, ZD 2018, 463 (467).; vgl. auch BVerfGE 120, 378.

hoben werden, nach dem Verwendungskontext keine Auswertungsabsicht besteht und eine solche Auswertung auch nicht im Nachhinein erfolgt.[84] Gegen eine verobjektivierende, den Verarbeitungskontext und Auswertungsabsicht nicht berücksichtigende Sichtweise[85] spricht, dass andernfalls der Anwendungsbereich erheblich ausgedehnt würde und damit dem Schutzziel besonders sensible und kritische Datenverarbeitungen zu steuern nicht Rechnung getragen würde.[86]

Besondere Kategorien personenbezogener Daten in Metadaten: Treten natürliche Personen in Kontakt mit KI-Systemen (bspw. einem Chat-Bot) können Metadaten anfallen.[87] Sind in den Metadaten Klarnamen und/oder Daten zum Geburts- oder Wohnort enthalten, können diese ebenfalls Angaben zur rassischer und ethnischer Herkunft ermöglichen.[88] Fraglich ist auch hier, ob der Name allein als rassische und ethnische Angabe zu sehen und somit als besondere Kategorie personenbezogener Daten zu betrachten ist. Zwar lässt sich möglicherweise schon allein aus dem Namen einer Person eine rassische oder ethnische Herkunft ableiten bzw. vermuten; dies sollte aber nur im Ausnahmefall bei Hinzutreten besonderer Umstände zur Anwendbarkeit des Art. 9 DSGVO führen.[89] Das Merkmal der „rassischen Herkunft" bezieht sich vor allem auf die biologische Abstammung und vererbbare Eigenschaften, während bei der „ethnischen Herkunft" eher der kulturelle Aspekt gemeint wird, der eine Menschengruppe kennzeichnet.[90] Dazu zählen besonders Sprache, Geschichte, Tradition, gemeinsame Werte, ein Zusammengehörigkeitsgefühl als Gruppe und die „sprachlichen und kulturellen Beziehung eines Menschen zu seinen Vorfahren".[91] Insgesamt wäre auch hier die Argumentation entsprechend der Bilddaten einschlägig: es kommt für die Sensibilität der Daten auf den Kontext der Datenverarbeitung an, also ob diese Angaben auch für eine Herkunftsanalyse bzw. -prognose genutzt werden.

2.2.4 Anonyme Daten

Die DSGVO selbst definiert die Anonymisierung nicht. Sie stellt allerdings klar, dass die DSGVO nicht für anonyme bzw. anonymisierte Daten anwendbar sein soll. Eine Definition der Anonymisierung findet sich hingegen in der Open-Data-Richtlinie.

> **ErwGr. 26, S. 5, 6 DSGVO** Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymen Daten, auch für statistische oder für Forschungszwecke.

[84] *European Data Protection Board*, Guidelines 3/2019 on processing of personal data through video devices, S. 14; *Schneider/Schindler*, ZD 2018, 463 (467).; vgl. auch BAG, Urteil vom 25.09.2013 - 10 AZR 270/12, Rn. 49 (zur alten Rechtslage).
[85] befürwortend: *Petri,* in: NK Datenschutzrecht Art. 9 Abs. 12.
[86] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 13; ähnlich *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 7.
[87] Unter Metadaten versteht man Daten, die ihrerseits dazu dienen, ausgewählte Aspekte von (Primär) Daten zu beschreiben, wie z. B. Telefonnummern und sonstige Kontaktdetails, Zeitpunkte bzw. Dauer einer Kommunikation sowie ggf. Standort der kommunizierenden Parteien, vgl. hierzu: *Krüger/Möllers*, MMR 2016, 728 (728); *Faas*, ArbRAktuell 2018, 594 (595); *Polst u. a.*, DuD 2021, 19 (20).
[88] *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 29; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 29.
[89] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 26; *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 7.
[90] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 16. *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 26.
[91] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 16; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 26; Beispiele auch bei: *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 16.

> **Art. 2 Nr. 7 RL (EU) 2019/1024** „Anonymisierung" den Prozess, in dessen Verlauf Dokumente in anonyme Dokumente umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten so anonym gemacht werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann

Gerade im Bereich intelligenter Datenauswertung und wachsenden Datenmengen stellt sich die Frage, wann rechtssicher von anonymen Daten ausgegangen werden kann.[92]

Keine absolute Anonymität erforderlich: Anonymisierung muss (Re-)Identifizierungsrisiken nicht „auf Null" reduzieren.[93] Ein solider Anonymisierungsprozess zielt darauf ab das Risiko der Re-Identifizierung unter einen bestimmten Schwellenwert zu senken. [94] Dieser Schwellenwert hängt laut EZ-Datenschutzbeauftragtem (EDSB) von mehreren Faktoren ab, wie zum Beispiel

- den bestehenden Risikominimierungsmaßnahmen,
- eventuell öffentlich verfügbarer Daten,
- die Auswirkungen auf die Privatsphäre des:der Einzelnen im Falle einer Re-Identifizierung, sowie
- den Motiven und der Fähigkeit eines potentiellen Angreifers zur Re-Identifizierung der Daten.[95]

Ob Daten anonym im Rechtssinne sind, hängt somit von der Bewertung der Restrisiken einer (Re-)Identifizierung ab.

Anonymisierung als kontinuierlicher Prozess: Die Abgrenzung personenbezogener und anonymer Daten stellt eine der wesentlichsten Herausforderungen des Datenschutzrechts dar. Insbesondere kann ein Datensatz durch ein identifizierendes Merkmal „infiziert" werden, sodass – auch wenn unbeabsichtigt – ein „Hineinwachsen" in den Personenbezug möglich ist.[96] Die Schwierigkeit bei der Bestimmung der Re-Identifizierungsrisiken liegt darin, dass bspw. durch fortschreitende Verknüpfung mit weiteren Datenbeständen (Stichwort Big Data) oder verbesserte Identifizierungstechniken, die Gefahr eines dynamischen „Hineinwachsens" in den Personenbezug droht.[97] Gerade die stetige Verbesserung der Rechenkapazität kann dazu führen, dass anonyme Datenbestände erneut bestimmten Personen zugeordnet werden können.[98] Weitere Risiken sind die Offenlegung weiterer Daten im Laufe der Zeit oder Datenpannen, die eine Verknüpfung zuvor anonymer Daten zu einer identifizierbaren Person ermöglichen können.[99] Die Übergänge zwischen anonymen und personenbezogenen Daten können folglich fließend und zeitvariabel sein, sodass Re-Identifizie-

[92] *Niemann/Kevekordes*, CR 2020, 17 (19 f.).
[93] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization; *Niemann/Kevekordes*, CR 2020, 17 (20).
[94] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.
[95] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.
[96] *Weichert*, DuD 2007, 113 (117); *Marnau*, DuD 2016, 428; *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (165); *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136; *Kühling/Klar*, ZD 2017, 27 (28).
[97] *Marnau*, DuD 2016, 428 (429); *Roßnagel*, ZD 2013, 562 (566); *Sarunski*, DuD 2016, 424 (427); *Boehme-Neßler*, DuD 2016, 419 (422); *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (165); *Raabe/Wagner*, DuD 2016, 434 (435); *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 35.
[98] *Karg*, DuD 2015, 520 (526). *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.
[99] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.

rungsrisiken stets bedacht werden sollten. Absehbare oder zu erwartende zukünftige Entwicklungen in Bezug auf Kontextwissen, Technik oder dem Wert der Informationen sollten daher antizipiert werden.[100] Empfohlen wird daher eine regelmäßige (Neu-)Bewertung der Verhältnismäßigkeit des Aufwands der De-Anonymisierung.[101]

Verschlüsselung als Anonymisierung? Nach Ansicht des EU-Datenschutzbeauftragten (EDSB) ist die Verschlüsselung keine Anonymisierungstechnik.[102] Zunächst verbleibt es bei der Möglichkeit der Entschlüsselung, sodass der Schlüssel als zusätzliche identifizierende Information zu werten ist. Es bestehen somit eher Parallelen zur Pseudonymisierung.[103] Selbst wenn dieser Schlüssel gelöscht wird, verbleiben weitere Faktoren auf lange Sicht, welche eine Entschlüsselung ermöglichen könnten.[104] Risiken der Rückgewinnung der Daten resultieren aus der Stärke des Verschlüsselungsalgorithmus und des Schlüssels selbst, Datenpannen, Problemen der Implementierung, der Menge der Verschlüsselten Daten, der Speicherdauer und der technologischen Entwicklung als auch dem Zweck der Datenvorhaltung. In unterschiedlichsten Kontexten werden Daten bspw. in gehashter Form verarbeitet. Das VG Bayreuth entschied hierzu, dass durch den Vorgang des Hashens die Daten nicht i.S.d. (damals noch einschlägigen) § 3 Abs. 6 BDSG a.F. anonymisiert würden, da es weiterhin mit nicht nur unverhältnismäßigem Aufwand möglich ist, sie einer bestimmten oder bestimmbaren Person zuzuordnen: „zumal andernfalls auch ein sich an die Übermittlung anschließender Datenabgleich seitens [des Anbieters] nicht möglich wäre."[105] Der EDSB scheint zudem davon auszugehen, dass Daten für alle Akteure entweder personenbezogen oder anonym sind.[106]

Praktische Umsetzung: In praktischer Hinsicht besteht die Möglichkeit, vorsorglich im Zweifel von einem Personenbezug auszugehen und die datenschutzrechtlichen Vorschriften zu beachten.[107] Auch wenn im allgemeinen Sprachgebrauch oftmals von „Anonymität im Netz" die Rede ist, sollte angesichts der Fülle anfallender Daten sowie insbesondere bei Notwendigkeit einer Zuordenbarkeit in vielen Bereichen eher von Pseudonymität gesprochen werden. Zu unterstreichen ist insoweit, dass es für die Einordnung als personenbezogen und damit die Anwendbarkeit der DSGVO nicht darauf ankommt, dass die betroffenen Personen namentlich bekannt sind. Nicht bei allen Daten kann das richtige Gleichgewicht zwischen der Verringerung des (Re-)Identifizierungsrisikos einerseits und der Nutzbarkeit des Datensatzes für den beabsichtigten Zweck andererseits gefunden werden.[108] Ist die Gesamtanzahl der unterschiedlichen Personen im Datensatz gering, bestehen oft Risiken, dass einzelne Personen herausgefiltert werden können.[109] Werden verschiedenste Kategorien von Daten verarbeitet, insbesondere eine große Anzahl demografischer Merkmale oder Standortdaten, steigt auch die Wahrscheinlichkeit, dass eine Information oder eine Kombination von Informationen aus

[100] *Hammer/Knopp*, DuD 2015, 503 (507); vgl. auch *Piltz*, K&R 2016, 557 (561).
[101] *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 35; *Roßnagel*, ZD 2018, 243 (247); *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 13; *Klar/Kühling,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 22.
[102] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.
[103] *Quiel/Kukin*, DSB 2022, 209 (209).
[104] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization. a.A. *Quiel/Kukin*, DSB 2022, 209 (210).
[105] VG Bayreuth, Beschluss vom 08.05.2018 – B 1 S 18.105 –, Rn. 47; bestätigt durch: Bayerischer Verwaltungsgerichtshof, Beschluss vom 26.09.2018 – 5 CS 18.1157 –, Rn. 11 ff.
[106] *Quiel/Kukin*, DSB 2022, 209 (209).
[107] *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (166 f.). Andere fordern wiederum die Steuerung von (Re-)Identifizierungsrisiken durch datenschutzrechtliche Vorsorgeregelungen: *Roßnagel/Scholz*, MMR 2000, 721 (728 ff.).
[108] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.; Quiel/Kukin, DSB 2022, 209 (210).
[109] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.

einer Masse von Daten eindeutig nur auf eine Person zutrifft.[110] Im Hinblick auf den Gedanken einer automatisierten Anonymisierung, gibt der EDSB zu bedenken, dass die Einschätzung der (Re-)Identifizierungsrisiken durch Eingreifen menschlicher Expertise unumgänglich ist.[111]

Der Einsatz von Anonymisierungstechniken kann allerdings auch dann noch im Rahmen der Rechtmäßigkeit einer Datenverarbeitung eine entscheidende Rolle spielen, wenn es sich weiterhin um personenbezogene Daten im Rechtssinne handelt, da hiermit Risiken für die Rechte und Freiheiten betroffener Personen minimiert werden.

Typische Fehlannahmen zur Anonymisierung[112]

Pseudonyme sind anonym
Verschlüsseln anonymisiert
Anonymisierung ist immer möglich
Einmal anonym immer anonym
Anonymisierung muss Identifizierung zu 100% verhindern
Anonymisierung ist nicht messbar
Anonymisierung ist vollständig automatisierbar
Anonymisierte Daten sind nutzlos
Anonymisierungsverfahren sind universell übertragbar
Niemand hat ein Interesse an De-Anonymisierung

2.2.5 Pseudonyme Daten

Anders als die Anonymisierung führt die Pseudonymisierung regelmäßig nicht zum Ausschluss des Personenbezugs und damit verbleibt es bei der Anwendbarkeit des Datenschutzrechts.[113] Definiert wird die Pseudonymisierung als:

> **Art. 4 Nr. 5 DSGVO „Pseudonymisierung“** die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

Zur Anwendbarkeit des Datenschutzrechts hebt ErwGr. 26 S. 2 DSGVO hervor:

[110] *Quiel/Kukin*, DSB 2022, 209 (210).
[111] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.
[112] *AEDP - agencia espanola protección datos/EDPS - European Data Protection Supervisor*, Joint paper on 10 misunderstandings related to anonymization.
[113] *Gausling*, DSRITB 2018, 519 (528); *Niemann/Kevekordes*, CR 2020, 17 (19).; *Köllmann*, NZA 2020, 831 (832); *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 40; *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 32; *Schmitz*, ZD 2018, 5 (6); a.A. *Roßnagel*, ZD 2018, 243 (244); *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 91.

> Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.

Die Pseudonymisierung ermöglicht gegenüber der Anonymisierung, dass Personen wiedererkennbar bleiben, ohne dass jedoch eine vollständige Identifikation möglich ist.[114] Ist eine Zuordnungsregel zwischen Pseudonym und Person bekannt, ist die Pseudonymisierung rücknehmbar, sodass wieder ein Personenbezug hergestellt werden kann.[115] Zudem gilt zu bedenken, dass häufig verwendete Pseudonyme auch einen Wiedererkennungseffekt gegenüber Dritten auslösen können. [116] Sie können – je nach konkreten Umständen – daher eine ähnlich identifizierende Wirkung haben, wie der Name. Folglich gilt die Pseudonymisierung zwar als eine Schutzmaßnahme, führt aber regelmäßig nicht zur Unanwendbarkeit des Datenschutzrechts.[117]

2.3 Zwischenfazit

Mit der Formulierung „alle Informationen“ in Art. 4 Nr. 1 DSGVO wird deutlich, dass der Anwendungsbereich des Datenschutzrechts sehr weit gefasst ist und die personenbezogenen Daten vielfältig sein können.[118] Irrelevant sind Fragen dazu, in welcher Form Informationen vorliegen, wie sie gespeichert sind, ob sie neu sind oder wie sensibel diese Daten sind.[119] Geschützt sind natürliche Personen, wobei Unternehmens- und Sachdaten je nach Kontext auch Rückschlüsse auf die dahinter stehende Person zulassen können. Zur genauen Abgrenzung hilft die Prüfung, ob sich Inhalt, Zweck oder Ergebnis der Datenverarbeitung auf eine bestimmte Person beziehen. Zur Feststellung, ob sich die Daten auf eine identifizierbare Person beziehen, müssen alle legal und mit verhältnismäßigem Aufwand zugänglichen Zusatzinformationen berücksichtigt werden – wobei sowohl aktuelle Technologien als auch technologische Entwicklungen berücksichtigt werden müssen. Daher sollten De-Anonymisierungsrisiken regelmäßig evaluiert werden, sofern eine Datenverarbeitung außerhalb des Anwendungsbereichs des Datenschutzrechts stattfinden soll. Sobald eine Identifizierung möglich ist, liegen personenbezogene Daten vor und das Datenschutzrecht wird anwendbar.

[114] *Probst*, in: Bäumler/von Mutius, Anonymität im Internet, S. 179 (185).
[115] *Köllmann*, NZA 2020, 831 (832).
[116] vgl. ErwGr. 30 DS-GVO; zu indirekt identifizierenden Kennnummern siehe beispielsweise: EuGH, Urteil vom 20. Dezember 2017 – C-434/16 – Nowak, Rn. 29; zu statischen IP-Adressen: EuGH, Urteil vom 19. Oktober 2016 – C-582/14 – Breyer, Rn. 36; *Golembiewski*, in: Bäumler/von Mutius, Anonymität im Internet, S. 107 (109); *Roßnagel/Scholz*, MMR 2000, 721 (727); *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 102. Zur Verkettbarkeit: *Hansen*, in: Bäumler/von Mutius, Anonymität im Internet, S. 198 (201).
[117] *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 40; *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 32; *Schmitz*, ZD 2018, 5 (6); a.A. *Roßnagel*, ZD 2018, 243 (244); *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 91.
[118] EuGH, Urteil vom 20.12.2017 – C-434/16 – Nowak, Rn. 33 ff. m.w.N.
[119] statt vieler: *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 8.

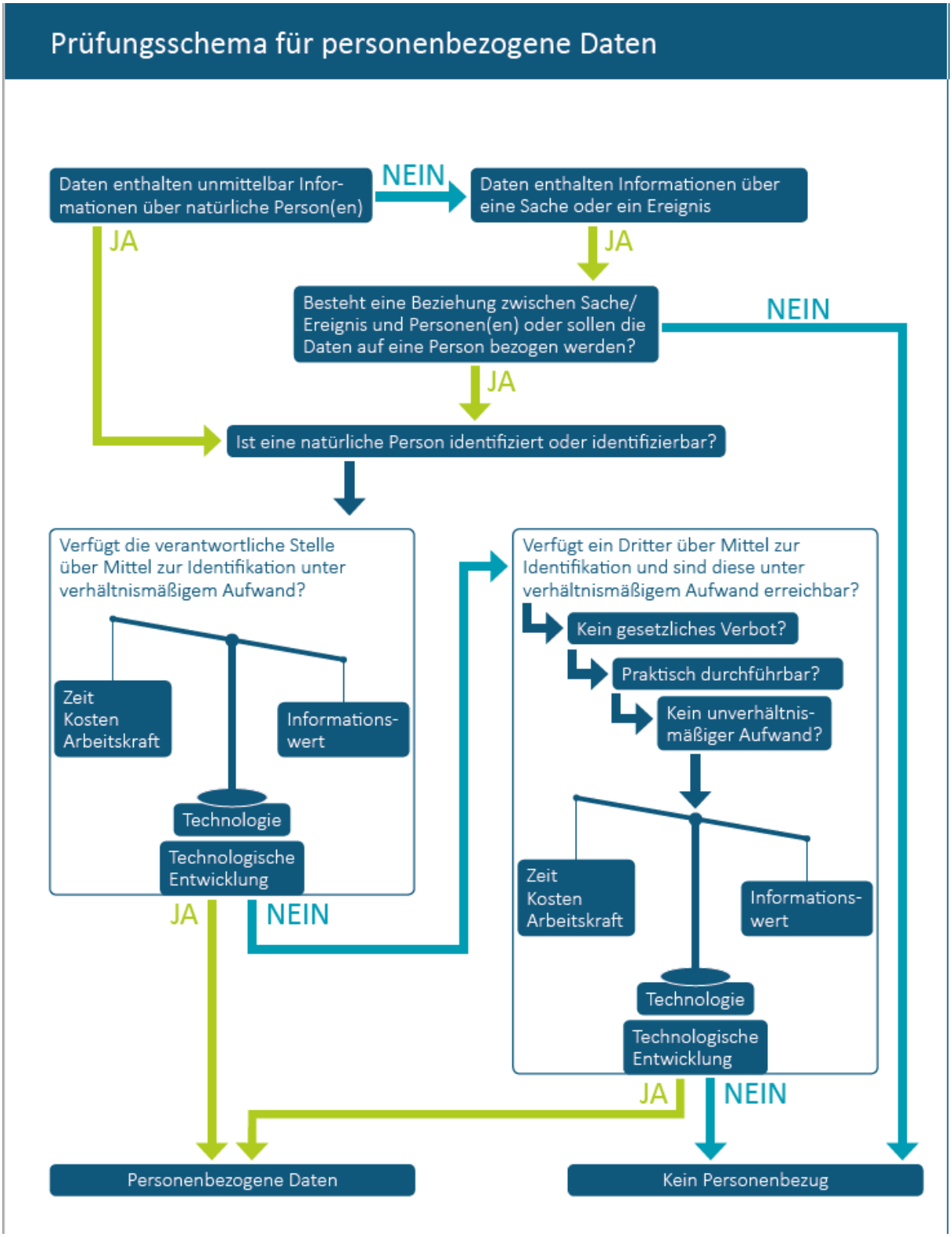


Abbildung 4 Prüfschema Personenbezug

3 Hintergrund: Grundrechtliche Schutzverbürgungen

Der Umgang mit diesen Daten unterliegt je nach spezifischer Fallkonstellation unterschiedlichen Schutzbedürfnissen, welche aus den Grundrechten als objektive Werteordnung herrühren. Das einfach-rechtliche Datenschutzrecht ist im Lichte dieser grundrechtlichen Gehalte auszulegen, weshalb im Vorgriff auf die Einzeldarstellung rechtlicher Vorgaben ein kurzer Überblick über die grundrechtlichen Schutzverbürgungen erforderlich ist.

Für Europa sind drei Grundrechtskataloge von herausragender Bedeutung: die Europäische Menschenrechtskonvention (EMRK), die EU-Grundrechtecharta (EU-GrCh) sowie die nationalen Verfassungsrechte, in Deutschland das Grundgesetz (GG).

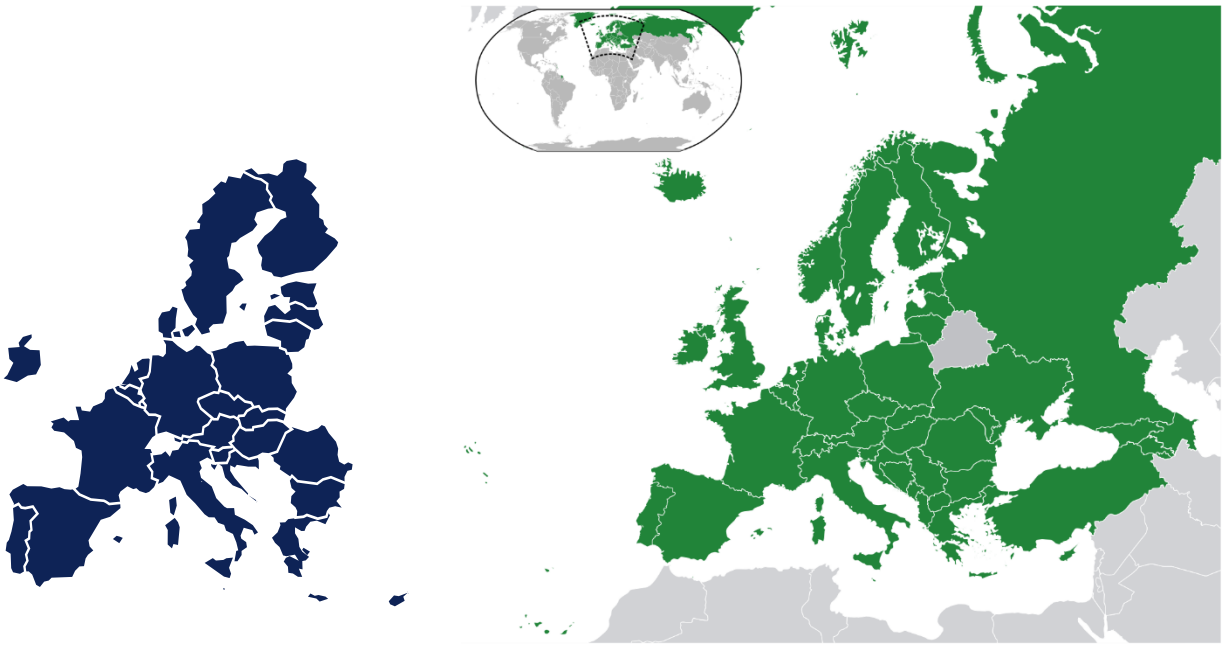


Abbildung 5 MItgliedstaaten der EMRK (grün)[120] und der EU (blau)

3.1 Betroffene Grundrechte

3.1.1 Technischer Imperativ und die Würde des Menschen

> **Art. 1 Abs. 1 GG** Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Der Einzug von KI-Systemen in unterschiedlichen Lebensbereichen und die damit einhergehende Automatisierung von Entscheidungen, die bisher der menschlichen Einflusssphäre unterlagen, wirft in der rechtwissenschaftlichen Diskussion die Frage nach der Vereinbarkeit mit der Menschenwürde auf.[121] Die Verdrängung

[120] Quelle: Von Hayden120 and NuclearVacuum - Location European nation states.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=8299320 [letzter Abruf 02.11.2021].

[121] Siehe bspw. zur Automatisierung des Straßenverkehrs: *Hilgendorf*, in: Hilgendorf/Hötitzsch/Lutz, Rechtliche Aspekte automatisierter Fahrzeuge: Beiträge zur 2. Würzburger Tagung zum Technikrecht im Oktober 2014, S. 15 (20 f.) m.w.N. *Wagner*, Das neue Mobilitätsrecht, S. 30 f.

des Menschen aus der Akteursrolle könnte als Angriff auf die Menschenwürde verstanden werden.[122] Im Rahmen der „Objektformel“ sind konkret spürbare Nachteile bei der jeweils betroffenen Person nicht konstituierend, da die Menschenwürde als solche bereits betroffen ist, wenn Menschen zum „Objekt, einem bloßen Mittel oder vertretbaren Größe herabgewürdigt“ werden.[123] Da Menschen stets Objekt der Verhältnisse, gesellschaftlichen Entwicklung oder des Rechts sind, muss hinzukommen, dass die Subjektqualität des Betroffenen grundsätzlich in Frage gestellt wird.[124] Schon mit der Formulierung von der „Unantastbarkeit“ in Art. 1 Abs. 1 S. 1 GG sowie der „Unveräußerlichkeit“ der Menschenrechte in Art. 1 Abs. 2 GG kommt zugleich deren grundsätzliche Unverlier- und Unverzichtbarkeit zum Ausdruck.[125] Im Hinblick auf umfassende Datenverarbeitung droht die Person ihre Würde zu verlieren, wenn sie aufgrund der aus Daten abgeleiteten oder ableitbaren Wissensmacht manipulierbar oder gar erpressbar wird.[126] Ein würdevolles Leben beinhaltet eine ureigenste Intimsphäre.[127] Nach der Rechtsprechung des BVerfG ist die Verletzung des sozialen Wert- und Achtungsanspruchs durch Kommerzialisierung menschlichen Daseins mit der Würde des Menschen ebenfalls grundsätzlich unvereinbar.[128]

Art. 1 EU-GrCh Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.

Vergleichbar zu Art. 1 Abs. 1 GG bekennt sich auch die EU-Grundrechtecharta zur unveräußerlichen Menschenwürde als fundamentalem Wert, auslegungsleitendem Leitbegriff und einklagbarem Grundrecht in Art. 1 EU-GrCh.[129] Bereits im Wortlaut offenbaren sich mit der Formulierung „zu achten und zu schützen“ die zwei grundlegenden Dimensionen des Grundrechtsschutzes als Abwehrrecht gegenüber Handlungen der Organe und Einrichtungen der Union und der Mitgliedstaaten einerseits und staatliche Schutzpflicht gegen Beeinträchtigung der Menschenwürde durch private Dritte andererseits.[130] Die Menschenwürde ist der soziale Wert- und Achtungsanspruch, der dem Menschen wegen seines Menschseins zukommt.[131]

Eine exakte Abgrenzung des Schutzbereichs gilt aufgrund der unterschiedlichen historischen Entwicklungen und rechtsphilosophischen Traditionen innerhalb der EU als besonders schwierig.[132] Die Konturierung des Schutzgehalts obliegt schlussendlich den Gerichten unterstützend durch wissenschaftliche Arbeiten. Im Rahmen der Forschung wird auch die Menschenwürde als tangiert angesehen, wenn im Rahmen der „Digitalisierung des menschlichen Lebens“ umfangreiche Datenanalysen eine umfassende Vermessung der menschlichen Persönlichkeit ermöglichen und damit immer effizientere Wege zur Steuerung von menschlichem Verhalten bedingen.[133]

[122] Ablehnend für den Straßenverkehr: *Hilgendorf*, in: Hilgendorf/Hötitzsch/Lutz, Rechtliche Aspekte automatisierter Fahrzeuge: Beiträge zur 2. Würzburger Tagung zum Technikrecht im Oktober 2014, S. 15 (20 f.); *Wagner*, Das neue Mobilitätsrecht, S. 30 f.
[123] *Dürig*, AöR 1956, 117 (127). Zur Objektformel: BVerfGE 27, 1-10 – Mikrozensus, Rn. 20; BVerfGE 30, 1-47 – Abhörurteil, Rn. 81; BVerfGE 45, 187-271 – lebenslange Freiheitsstrafe, Rn. 145; BVerfGE 87, 209-233 – Tanz der Teufel, Rn. 107; BVerfGE 109, 279-391 – großer Lauschangriff, Rn. 121; BVerfGE 115, 118-166 – Luftsicherheitsgesetz, Rn. 119.
[124] BVerfGE 109, 279-391 – großer Lauschangriff, Rn. 121.
[125] *Dürig*, AöR 1956, 117 (117); *Hillgruber,* Epping/Hillgruber, BeckOK GG Art. 1 Rn. 74; *von Lewinski*, Die Matrix des Datenschutzes, S. 54.
[126] *Masing*, RDV 2014, 3 (4).
[127] BVerfGE 27, 1-10 – Mikrozensus, Rn. 21; *Dürig*, AöR 1956, 117 (129).
[128] BVerfG, Beschluss vom 12.11.1997 – 1 BvR 479/92 – Kind als Schaden, Rn. 67.
[129] *Callies,* in: Callies/Ruffert, EUV/AEUV Art. 1 Rn. 2; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 1 Rn. 2.
[130] *Callies,* in: Callies/Ruffert, EUV/AEUV Art. 1 Rn. 5 m.w.N.
[131] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 1 Rn. 6.
[132] *Callies,* in: Callies/Ruffert, EUV/AEUV Art. 1 Rn. 19.
[133] *Erdmannsdorff, von*, MMR 2021, 700.

3.1.2 Persönlichkeitsschutz und Datenschutzgrundrechte

Im engen Zusammenhang zur Menschenwürdegarantie stehen Aspekte der Persönlichkeitsentfaltung, Selbstbestimmung und mit besonderem Blick auf Digitalisierung und Einsatz Künstlicher Intelligenz: der Datenschutz.

3.1.2.1 Datenschutz und die Schutzgutdebatte

Obwohl der Schutzgegenstand oftmals schlicht als das „personenbezogene Datum“ beschrieben wird,[134] darf Datenschutz nicht mit dem „Schutz der Daten“ verkürzt werden, sondern hat generell den Schutz des Menschen bei der Datenverarbeitung zum Gegenstand.[135] Das Datum i.S.d. der Informationswissenschaft fungiert praktisch nur als objektiver Anknüpfungspunkt zur Regulierung der Informations- und Wissenserzeugung in Handlungs- und Entscheidungszusammenhängen.[136] Im Hinblick auf die konkrete konzeptionelle Eingrenzung des Schutzguts der informationellen Selbstbestimmung herrscht allerdings seit dem Volkszählungsurteil ein dogmatischer Streit zwischen einer primär datenzentrierten, eigentumsähnlichen Schutzkonzeption im Sinne des „meine Daten gehören mir“[137] auf der einen Seite und einem auf autonome Entfaltungsfreiheit gerichteten Schutz auf der anderen Seite.[138] Dieser Streit gewinnt an Komplexität, wenn man die Aufteilung in ein Grundrecht auf Achtung des Privatlebens (Art. 7 EU-GrCh) und ein Grundrecht auf Schutz personenbezogener Daten (Art. 8 EU-GrCh) in der EU-Grundrechtecharta betrachtet. Im Hinblick auf die neuen Bedrohungen durch den Einsatz von KI-Systemen – wie Diskriminierung, Manipulation und Fremdbestimmung durch algorithmisch-maschinelle Entscheidungen sowie deren automatisierte Durchsetzung bis hin zur direkten oder indirekten Steuerung der betroffenen Person, wird deutlich, dass die Regulierung der Datenverarbeitung einen Vorfeldschutzcharakter hat.[139] Die typische Gefahr für die Freiheit des Individuums liegt nicht ausschließlich im Zugang zu Daten, sondern vor allem in den Möglichkeiten der Veredelung von Daten zu Wissen sowie offenen oder verdeckten Entscheidungen und damit nicht nur im Ausspähen und Bloßstellen bzw. der Sorge davor, sondern auch in der allgegenwärtigen Präformation durch Fremderwartungen. [140] Denn das Ziel des allgemeinen Persönlichkeitsrechts liegt in der Gewährleistung von Grundlagen zur Selbstentfaltung des Einzelnen, wofür es erforderlich ist, in gewissem Umfang regelbar und vorhersehbar zu machen, welche Daten überdauern und einem später vorgehalten werden können.[141]

---

[134] Vgl. *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (16); *Specht*, CR 2016, 288 (290).

[135] Bundestags-Drucksache 7/1027, S. 14; *von Lewinski*, Die Matrix des Datenschutzes, S. 4; ähnlich *Sahl*, RDV 2015, 236 (239); *Grimm*, JZ 2013, 585 (585); *Schnabel*, ZUM 2008, 657 (657); a.A. wohl *Specht*, CR 2016, 288 (290).

[136] *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (26).

[137] *Fetzer*, MMR 2015, 777 (778); *Künast*, ZRP 2008, 201 (201); *Krönke*, Der Staat 2016, 319 (342); ähnlich *Wandtke*, MMR 2017, 6 (9); *Bräutigam*, MMR 2012, 635 (639). Entsprechend der informationswissenschaftlichen Terminologie müsste der Ausspruch korrekt lauten: »Daten, Informationen und Wissen über mich gehören mir«.

[138] *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (26); *Britz*, EuGRZ 2009, 1 (8); *Bäcker*, Der Staat 2012, 91 (95); *Boehme-Neßler*, International Data Privacy Law 2016, 222 (223); *Denninger*, in: Bäumler/von Mutius, Anonymität im Internet, S. 41 (49); *Giesen*, CR 2014, 550 (552); *Grimm*, JZ 2013, 585 (585); *Gurlit*, NJW 2010, 1035 (1036); *Hermstrüwer*, Informationelle Selbstgefährdung, S. 32; *Klement*, JZ 2017, 161 (162); *Masing*, RDV 2014, 3 (4); vgl. auch *von Lewinski*, Die Matrix des Datenschutzes, S. 44.

[139] BVerfGE 120, 274-350 – Online-Durchsuchung, Rn. 198; BVerfGE 120, 378-433 - automatisierte Kennzeichenerfassung, Rn. 64; BVerfGE 120, 351-377 – Rasterfahndung, Rn. 57; BVerfGE 118, 168-211 – Kontenabfrage, Rn. 87; BVerfGE 115, 320-381 – Rasterfahndung, Rn. 70; BVerfGE 113, 29 – Beschlagnahme von Datenträgern, Rn. 82; *Bäcker*, Der Staat 2012, 91 (96); *Bull*, NJW 2006, 1617 (1622); *Grimm*, JZ 2013, 585 (586); *Krönke*, Der Staat 2016, 319 (343); *Heilmann*, Anonymität für User-Generated Content?, S. 91; *Masing*, RDV 2014, 3 (4); *Sahl*, RDV 2015, 236 (239); *von Lewinski*, Die Matrix des Datenschutzes, S. 78; ähnlich *Ruppel*, Persönlichkeitsrechte an Daten?, S. 32.

[140] Britz, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 561 (567); Härting/Schneider, CR 2015, 819 (820).

[141] Masing, RDV 2014, 3 (4); Bäcker, Der Staat 2012, 91 (95).

3.1.2.2 Schutz des Privat- und Familienlebens in Europa

Datenschutzgrundrechte existieren sowohl auf nationaler als auch auf internationaler Ebene und haben damit unterschiedliche Reichweite. Die älteste Regelung zum Datenschutz als Menschenrecht gewährt die Europäische Menschenrechtskonvention (EMRK), welche durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) stetig angepasst und an aktuelle Herausforderungen fortentwickelt wird.

> **Art. 8 EMRK**
>
> (1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
>
> (2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Der Schutz des Privat- und Familienlebens wurde dabei vom EGMR weit ausgelegt, indem mehrfach betont wurde, dass eine abschließende Definition des „Privatlebens“ nicht möglich ist.[142] Dabei unterstrich das Gericht in seinen Entscheidungen sowohl die Aspekte der Selbstbestimmung[143] als auch des Datenschutzes[144]. Aus dem Grundrecht folgerte der EGMR zudem eine staatliche Handlungspflicht, wonach Vertragsstaaten ausreichende Garantien gegen Datenmissbrauch vorsehen müssen.[145]

In Deutschland genießt die EMRK zwar nur den Rang eines einfachen Gesetzes, wird aber bei Auslegung der nationalen Grundrechte als wichtige Rechtserkenntnisquelle herangezogen.[146] Ebenfalls hatte sie einen entscheidenden Vorbildcharakter für die Entwicklung eines eigenständigen EU-Grundrechtskatalogs.[147]

---

[142] EGMR, Urteil vom 19.02.2015 – 53649/09 – Ernst August von Hannover/Deutschland, Rn. 44; EGMR Urteil vom 29.04.2002 - 2346/02 - Pretty/UK, Rn. 61; EGMR, Urteil vom 2.09.2010 – 35623/05 - Uzun/Deutschland, Rn. 43; EGMR, Urteil vom 20.01.2011 – 31322/07, NJW 2011, 3773 – Haas/Schweiz, Rn. 50; EGMR, Urteil vom 23.09.2010 – 425/03– Obst/Deutschland, Rn. 39; EGMR, Urteil vom 16.02.2000 – 27798/95 – Amann/Schweiz, Rn. 65; EGMR, Urteil vom 25.09.2001, 44787/98 - P.G. u. J.H./UK, Rn. 56; EGMR, Urteil vom 28.04.2003 – 44647/98 – Peck/UK, Rn. 57; EGMR, Urteil vom 17.10.2003 – 63737/00 – Perry/UK, Rn. 36; EGMR, Urteil vom 23.09. 2010 – 1620/03 – Schuth/Deutschland, Rn. 53; EGMR, Urteil vom 12.06.2014 – 56030/07– Fernandez Martinez/Spanien, Rn. 109.

[143] EGMR, Urteil vom 19.07.2012 – 497/09 - Koch/Deutschland, NJW 2013, 2953; EGMR, Urteil vom 20.01.2011 – 31322/07, NJW 2011, 3773 – Haas/Schweiz; EGMR, Urteil vom 23.09.2010 – 425/03 – Obst/Deutschland, Rn. 39; EGMR, Urteil vom 23.09. 2010 – 1620/03– Schuth/Deutschland; EGMR, Urteil vom 12.06.2014 – 56030/07 – Fernandez Martinez/Spanien, Rn. 110; EGMR, Urteil vom 29.04.2002 – 2346/02 – Pretty/UK, NJW 2002, 2851.

[144] EGMR, Urteil vom 22.02.2018 – 588/13 – Libert/France, ZD 2018, 263; EGMR, Urteil vom 2.09.2010 – 35623/05 – Uzun/Deutschland, NJW 2011, 1333; EGMR, Urteil vom 29.06.2006 – 54934/00 – Weber u. Saravia/Deutschland, NJW 2007, 1433; EGMR, Urteil vom 4.12.2008 – 30562/04 – Marper/UK; EGMR, Urteil vom 16.02.2000 – 27798/95 – Amann/Schweiz; EGMR, Urteil vom 25.09.2001, 44787/98 – P.G. u. J.H./UK; EGMR, Urteil vom 28.04.2003 – 44647/98 – Peck/UK; EGMR, Urteil vom 17.10.2003 – 63737/00 – Perry/UK; EGMR, Urteil vom 26.03.1987 – 9248/81 – Leander/Schweden, Rn. 48; EGMR, Urteil vom 4.05.2000 – 28341/95 – Rotaru/Rumänien; EGMR, Urteil vom 03.04.2007 – 62617/00 – Copland/UK.

[145] Meyer-Ladewig/Nettesheim, in: HK-EMRK Art. 8 Rn. 32.

[146] BVerfG, Beschluss vom 26.02.2008 – 1 BvR 1602/07 – Caroline von Monaco III, Rn. 53; BVerfGE 111, 307, Rn. 30; BVerfGE 128, 326, Rn. 87; BVerfGE 74, 358-380, Rn. 35; BVerfGE 82, 106-126, Rn. 33; Kingreen/Poscher, Grundrechte, S. 20 Rn. 66/67; Kirchhof, NJW 2011, 3681 (3683).

[147] Boehm/Andrees, CR 2016, 146 (148); Boehm/Cole, ZD 2014, 553 (554); Britz, EuGRZ 2009, 1 (6f.); Michl, DuD 2017, 349 (350); Marsch, Das europäische Datenschutzgrundrecht, Kap. 1.

3.1.2.3 Dualismus aus Privatlebensschutz und Datenschutz in der EU

> **Art. 7 EU-GrCh Achtung des Privat- und Familienlebens**
>
> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.
>
> **Art. 8 EU-GrCh Schutz personenbezogener Daten**
>
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Auf Europäischer Ebene wurde mit der Etablierung eines eigenen Grundrechtskatalogs mit der Charta der Grundrechte der Europäischen Union (GrCh) europaweit ein Regelwerk geschaffen, dass Primärrechtsrang und somit dieselbe Gültigkeit wie der unionsrechtliche Vertrag von Lissabon selbst genießt. Die EU-Grundrechte kommen bei der „Durchführung des Rechts der Union“ zur Anwendung (vgl. Art. 51 EU-GrCh). Der Europäische Gerichtshof (EuGH) und das Bundesverfassungsgericht (BVerfG) befinden sich in einem kontroversen Dialog über die Reichweite des jeweiligen Grundrechtsregimes.[148] Dies hat zwar zentrale Auswirkungen auf die Zuständigkeit der Gerichte, aufgrund der weitreichenden Harmonisierung aber keine überbordenden Effekte für die Ebene der Anwendung und Auslegung des einfachen Rechts. Einige Gerichte bemühen die nationalen und europäischen Grundrechtskataloge gemeinsam.[149]

Auch das Verhältnis zwischen Art. 7 EU-GrCh und seinem „moderneren“ kleinen Bruder Art. 8 EU-GrCh ist höchst umstritten.[150] Einige sehen in „dem“ Datenschutzgrundrecht gegenüber Art. 7 GrCh, der u.a. das Recht auf Achtung des Privatlebens und der Kommunikation normiert, als lex specialis an.[151] D.h. dass Art. 8 GrCh als speziellere Vorschrift der allgemeineren Vorschrift in Art. 7 GrCh vorgehen würde. Der EuGH prüft dagegen beide Normen regelmäßig parallel und gleichrangig.[152]

Eine wesentliche Weichenstellung ist die Tatsache, dass der EuGH jede Verarbeitung personenbezogener Daten durch Dritte als einen Eingriff in den Schutzbereich wertet.[153] Für die Rechtfertigung sind dann wiederum die in Art. 8 Abs. 2 EU-GrCh aufgeführten Grundsätzen von elementarer Bedeutung.

---

[148] EuGH, Urteil vom 26. Februar 2013, Akerberg Fransson, C-617/10, EU:C:2013:105, Rn. 29; siehe auch EuGH, Urteil vom 26. Februar 2013, Melloni, C-399/11; BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08 –, Rn. 183; BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II.

[149] Sofern die materiellen verfassungsrechtlichen Wertungen sachgerecht eingestellt werden, sei den Anforderungen des Grundrechtsschutzes genügt: BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II, Rn. 124.

[150] Zum Streit siehe: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 216 ff. m.w.N.

[151] Statt vieler: *Bernsdorff,* in: Meyer, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 13; *Kingreen,* in: Callies/Ruffert, EUV/AEUV Art. 8 Rn. 1a.

[152] EuGH, Urteil vom 9.11.2010, C-92/09 und C-93/09 – Volker und Markus Schecke und Eifert, Rn. 47 ff.; EuGH, Urteil vom 13.05.2014, C-131/12 – Google Spain, Rn. 69 ff.; EuGH, Urteil vom 8.04.2014, C-293/12 und C-594/12 – Digital Rights Ireland, Rn. 29 ff.; EuGH, Urteil vom 21.12.2016, C-203/15 und C-698/15 – Tele2 Sverige Rn. 93, 129; EuGH, Urteil vom 6.10.2015, C- 362/14 – Schrems, Rn. 39 ff.

[153] EuGH, Urteil vom 08.04.2014 – C-293/12 – Digital Rights Ireland, Rn. 36; EuGH, Urteil vom 17.10.2013 – C-291/12 – Schwarz, Rn. 25; EuGH, Urteil vom 21.12.2016 – C-203/15 und C-698/15 – Tele2 Sverige, Rn. 100; *Franzen,* in: Franzen/Gallner/Oetker, EuArbR Art. 8 GRC Rn. 7; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 8; *Gersdorf,* in: BeckOK InfoMedienR Art. 8 EU-GrCharta Rn. 18; *Bieker*, DuD 2018, 27 (28); *Roßnagel*, NJW 2019, 1 (2).

3.1.2.4 Ausprägungen des Allgemeinen Persönlichkeitsrechts (APR) in Deutschland

Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG Recht auf informationelle Selbstbestimmung

BVerfGE 65, 1 - Volkszählungsurteil

- Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. […]

Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

BVerfGE 120, 274 - Onlinedurchsuchung

- Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. […]

In Deutschland hat das BVerfG in seinem wegweisenden Volkszählungsurteil aus dem Allgemeinen Persönlichkeitsrecht (APR) das Recht auf informationelle Selbstbestimmung abgeleitet.[154] Nach der Entscheidung des Gerichtes ist darunter die Befugnis des Einzelnen zu verstehen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[155] Das BVerfG hat damit einen Teilbereich des APR im Lichte der informationstechnischen Entwicklung interpretiert.[156] Konkretisiert und fortentwickelt wurde dieses Grundrecht im Lauf der Jahre durch weiteren Entscheidungen des BVerfG.[157]

Flankiert wird dieses klassische Datenschutzgrundrecht seit 2008 durch das ebenfalls aus dem APR entwickelten „Computergrundrecht“, dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme.[158] Aus verfassungsrechtlicher Perspektive erkennt das BVerfG ein erhebliches Schutzbedürfnis, welches aus der Angewiesenheit auf die Nutzung informationstechnischer Systeme folgt, für die Freiheitsverwirklichung und die allgemeine Entfaltung der Persönlichkeit an.[159] Auch juristische Personen können sich grundsätzlich nach Art. 19 Abs. 3 GG auf dieses Grundrecht berufen.[160]

3.1.3 Fernmeldegeheimnis und elektronische Kommunikation

Verbürgungen vor ausforschender oder missbräuchlicher Datenerfassung finden sich neben den klassischen Datenschutzgrundrechten auch als Teilaspekte in unterschiedlichen Grundrechten.[161] In Anbetracht der Tatsache, dass Menschen auf die Nutzbarkeit informationstechnischer Infrastrukturen im Informationszeitalter

[154] BVerfGE 65, 1 – Volkszählungsurteil.
[155] BVerfGE 65, 1 (43) – Volkszählungsurteil.
[156] Zur Entwicklung des Allgemeinen Persönlichkeitsrechts: BGHZ, 13, 334 – Leserbrief; BVerfGE 34, 238; BVerfGE 34, 269 – Soraya; BVerfGE 30, 173 – Mephisto; BVerfGE 27, 1 – Mikrozensus.
[157] Vgl. etwa BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II.
[158] BVerfGE 120, 274-350 - Online-Durchsuchung.
[159] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 33.
[160] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 21.
[161] *Masing*, RDV 2014, 3 (3); *Geminn/Roßnagel*, JZ 2015, 703 (703); vgl. auch *Gurlit*, NJW 2010, 1035 (1036f.).

angewiesen sind und ihre Alltagsgegenstände zunehmend im Internet der Dinge (IoT) vernetzt sind, geraten als besonders geregelte Garantien der Privatheit das Post- und Fernmeldegeheimnis nach Art 10 Abs. 1 GG[162] und der Schutz in der Wohnung nach Art. 13 Abs. 1 GG[163] ebenfalls in den Fokus der Betrachtung. Im Hinblick auf die Kommunikation im Unternehmenskontext ist das Fernmeldegeheimnis von besonderem Interesse.

> **Art. 10 Abs. 1 GG** Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
>
> **Art. 10 Abs. 2 GG** Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Mit dem Fernmeldegeheimnis nach Art. 10 Abs. 1 Var. 3 GG wird die körperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs geschützt.[164] Die Grundintention dieses Rechts liegt in der freien Entfaltung der Persönlichkeit und Würde des Menschen über die Abschirmung des Kommunikationsinhalts sowie Gewährleistung der Vertraulichkeit der näheren Kommunikationsumstände.[165] Dazu werden Daten über das Ob, die Zeitpunkte, die Kommunikationspartner sowie Anzahl der durchgeführten sowie versuchten Kommunikationsvorgänge gezählt.[166] Nicht unter diesem Gesichtspunkt verfassungsrechtlich geschützt ist anderseits das Vertrauen in die Integrität des Kommunikationspartners.[167] Der primäre Schutzzweck liegt in den Risiken des technischen Übermittlungsvorgangs begründet, den die Grundrechtsträger*innen anders als im Gespräch unter Anwesenden schlechter kontrollieren können und endet daher mit Abschluss des Übermittlungsvorgangs.[168]

3.1.4 Von KI-Systemen potentiell betroffene Grundrechte

Im April 2021 legte die EU-Kommission einen Verordnungsentwurf für eine KI-Regulierung (AI Act / Gesetz über künstliche Intelligenz) vor.[169] Als Schutzziele anhand deren sich das Risiko des KI-Systems messen lassen soll, werden vor allem die Allgemeininteressen, wie einem hohen Schutz der „Gesundheit, der Sicherheit

[162] BVerfGE 130, 151-212 – Bestandsdatenspeicherung, Rn. 111 ff.; BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 66; BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 – Telekommunikationsüberwachung, Rn. 80 ff.; BVerfGE 110, 33-76 – Außenwirtschaftsgesetz, Rn. 100 ff.; BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 – Telekommunikationsüberwachung, Rn. 160 ff.; BVerfGE 67, 157-185 - Post- und Telefonkontrolle – G10, Rn. 42 ff.

[163] BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 116 ff.; BVerfGE 109, 279-391 – großer Lauschangriff, Rn. 124; BVerfGE 51, 97-115 – Durchsuchungsanordnung, Rn. 22 ff.; *Becker*, JZ 2017, 170 (175).

[164] BVerfGE 67, 157 (172); BVerfGE 106, 28 (35 f.).

[165] BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 64; BVerfGE 110, 33-76 – Außenwirtschaftsgesetz, Rn. 101; BVerfGE 67, 157-185 - Post- und Telefonkontrolle – G10, Rn. 43.

[166] BGH, Urteil vom 13. Juli 2017 – I ZR 193/16 –, Rn. 15; BVerfGE 130, 151-212 – Bestandsdatenspeicherung, Rn. 112; BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 – Vorratsdatenspeicherung, Rn. 189; BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 72; BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 – Telekommunikationsüberwachung, Rn. 163; *Gurlit*, NJW 2010, 1035 (1036).

[167] *Apel*, ZD 2018, 486 (486); *Nettesheim*, VVDStRL 2011, 7 (22).

[168] BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 77; BVerfGE 106, 28-51 – Mithörvorrichtung, Rn. 22; BVerfGE 85, 386-405 – Fangschaltung, Rn. 46; *Gurlit*, NJW 2010, 1035 (1036).

[169] 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, Brüssel, den 21.4.2021, COM/2021/206 final.

und der Grundrechte“ genannt (vgl. ErwGr. 1, 5). Des Weiteren führt die EU-Kommission in ihrem Entwurf folgende Individualrechte und gruppenspezifische Rechte aus der EU-Grundrechtecharta[170] auf:

3.1.4.1 Individualrechte

Würde des Menschen (Art. 1): siehe Abschnitt 3.1.1.

Achtung des Privatlebens und Schutz personenbezogener Daten (Art. 7, 8): siehe Abschnitt 3.1.13.1.2.

Nichtdiskriminierung (Art. 21): Das allgemeine Diskriminierungsverbot listet Diskriminierungsmerkmale, die zum Teil auf Vorgaben des internationalen Rechts und teilweise auf gemeinsamen Verfassungsüberlieferungen der EU-Staaten beruhen.[171] Bei den Merkmalen handelt es sich um personengebundene Merkmale, auf die deren Träger regelmäßig keinen oder nur begrenzten Einfluss haben, sodass auch ein enger Zusammenhang zum Schutz der Menschenwürde besteht.[172]

> (1) Diskriminierungen, insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung, sind verboten.
>
> (2) Unbeschadet besonderer Bestimmungen der Verträge ist in ihrem Anwendungsbereich jede Diskriminierung aus Gründen der Staatsangehörigkeit verboten.

Vom Schutzbereich sind neben natürlichen Personen auch juristische Personen / Personengesellschaften erfasst, sofern Differenzierungsmerkmale auf sie anwendbar sind (bspw. die Staatsangehörigkeit).[173] Der Gleichheitsgrundsatz wurde im Sekundärrecht insbesondere in der allgemeinen Gleichbehandlungsrichtlinie 2000/78/EG umgesetzt, die zu einer horizontalen innerstaatlichen Anwendung führt.[174]

Im Rahmen einer Rechtfertigung kann zwischen unmittelbarer und mittelbarer[175] Diskriminierung differenziert werden: gerade im Arbeitsrecht finden sich Regelungen, die eine Ungleichbehandlung erforderlich machen können (bspw. Art. 4, 6 RL 2000/78/EG), im Übrigen gilt die Verhältnismäßigkeitsprüfung.[176]

Gleichheit von Frauen und Männern (Art. 23): Der in einem eigenen Artikel nochmals hervorgehobene Gleichheitssatz für die Geschlechtergleichheit enthält gleichzeitig einen Schutzauftrag sowie besonderen Rechtfertigungsgrund zum Abbau von Ungleichbehandlung (umgekehrte Diskriminierung).[177]

[170] Im durch EU-Recht determinierten Bereich sind die Grundrechte der EU-Grundrechtecharta maßgeblich, vgl. Art. 51 EU-GrCh. Vergleichbare Grundrechtsgehalte finden sich auch im GG, sollen an dieser Stelle allerdings nicht im Einzelnen dargestellt werden.
[171] *Hölscheidt,* in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union Art. 21 Rn. 2.
[172] *Rossi,* in: Callies/Ruffert, EUV/AEUV Art. 21 Rn. 3.
[173] *Rossi,* in: Callies/Ruffert, EUV/AEUV Art. 21 Rn. 4.
[174] EuGH, Urteil vom 27.07.2016 – C-414/16, ECLI:EU:C:2018:257, Rn. 76 ff. (Egenberger).
[175] Anknüpfen an vermeintlich neutralen Kriterien, die sich faktisch diskriminierend auswirken.
[176] *Rossi,* in: Callies/Ruffert, EUV/AEUV Art. 21 Rn. 10.
[177] *Hölscheidt,* in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union Art. 23 Rn. 15.

> Die Gleichheit von Frauen und Männern ist in allen Bereichen, einschließlich der Beschäftigung, der Arbeit und des Arbeitsentgelts, sicherzustellen.
>
> Der Grundsatz der Gleichheit steht der Beibehaltung oder der Einführung spezifischer Vergünstigungen für das unterrepräsentierte Geschlecht nicht entgegen.

Recht auf Meinungsfreiheit (Art. 11), Recht auf Versammlungs- und Vereinigungsfreiheit (Art. 12): Gerade der KI-Einsatz im Zusammenhang mit der Gesichtserkennung im öffentlichen Raum bedingt die Gefahr, dass Grundrechte wie die freie Meinungsäußerung und Versammlungsfreiheit nicht mehr wahrgenommen werden, wenn die Erwartung besteht, sich im öffentlichen Raum nicht mehr anonym aufhalten zu können.[178] So kann der Einsatz von Identifizierungssystemen bei Demonstrationen eine abschreckende Wirkung haben, wodurch Personen aus Angst negativer Folgen an der rechtmäßigen Ausübung ihrer Grundrechte gehindert werden.[179] In den Ethik-Leitlinien für eine vertrauenswürdige KI der Hochrangigen Expertengruppe wird zudem auf die Möglichkeit vieler unerwarteter psychologischer und soziokultureller Auswirkungen automatischer Identifizierung hingewiesen.[180]

Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht und die Unschuldsvermutung und Verteidigungsrechte (Art. 47, 48) sowie der allgemeine Grundsatz guter Verwaltung: Kommt es zum Einsatz Künstlicher Intelligenz bei juristischer Entscheidungsfindung, bestehen tiefgreifende Bedenken nicht nur im Hinblick auf die technische Reife und ethischer Fragen, sondern auch in verfassungsrechtlicher Hinsicht.[181] Der Einsatz algorithmischer Systeme durch Hoheitsträger wird als besonders sensibel eingestuft, sodass eine umfassende Risikofolgenabschätzung angemahnt wird.[182] So kann danach differenziert werden, ob natürliche oder juristische Personen des Privatrechts (z.B. Anwält*innen) bei ihrer Meinungsbildung KI-Systeme zur Hilfe nehmen und dabei das Ergebnis verantworten, oder ob KI in Richterfunktionen Einfluss auf die Entscheidungsfindung hat.[183] Auch in Deutschland besteht das Recht auf einen gesetzlichen Richter (Art. 101 Abs. 1 S. 2 GG), wobei das Richteramt zunächst eine natürliche Person impliziert.[184] Eine „automatisierte" Gerichtsentscheidung eines „Robo-Judge"[185] ist damit ausgeschlossen.[186] Gerade die Notwendigkeit der Bewertung von Unsicherheiten auf Sachverhaltsebene und die Auslegung unbestimmter Rechtsbegriffe, Vornahme von Wertungen, Abwägungen und Verhältnismäßigkeitsprüfungen, sowie Nutzung von „Entscheidungskorridoren" zeigt, dass der Mensch hier nicht einfach durch formale Logik mit binären Aussagen ersetzt werden kann.[187]

„Intelligenten" Algorithmen, die den Prozessstoff erfassen, einschlägige Literatur und Urteile auswerten, mit Entscheidungsdatenbanken abgleichen, bis hin dazu einen Entscheidungs- bzw. Verfahrensvorschlag zu un-

[178] *Lachenmann/Meyer*, MMR-Aktuell 2021, 440578 (3.).
[179] *Agentur der Europäischen Union für Grundrechte*, Gesichtserkennungstechnologien: grundrechtsrelevante Erwägungen im Rahmen der Strafverfolgung, S. 38.
[180] *Hochrangige Expertengruppe für Künstliche Intelligenz (HEG-KI) u. a.*, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 44.
[181] *Steinrötter/Warmuth,* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht Teil 30 Legal Tech Rn. 63.
[182] *Datenethikkommission der Bundesregierung*, Gutachten der Datenethikkommission, S. 30 Handlungsempfehlungen Nr. 68, 69.
[183] *Enders*, JA 2018, 721 (723).
[184] *Enders*, JA 2018, 721 (723).; vgl. auch *Stein, vom*, NZA 2021, 1057 (1060).
[185] Vgl. zum Konzept: *Steinrötter/Warmuth,* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht Teil 30 Legal Tech Rn. 61.; aufklärend über die Legende eines „Robo-Richters" in Estland: *Herberger,* beck-aktuell 10.09.2021, abrufbar unter: https://rsw.beck.de/aktuell/daily/magazin/detail/keine-robo-richter-in-estland [letzter Abruf am 01.07.2022].
[186] *Enders*, JA 2018, 721 (723).
[187] *Steinrötter/Warmuth,* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht Teil 30 Legal Tech Rn. 64 f.

terbreiten, wird das Potential beigemessen, die Qualität von Gerichtsurteilen zu verbessern und Entscheidungen einheitlicher und transparenter zu gestalten.[188] Aber auch bei der Vorbereitung der Entscheidungsfindung bestehen Bedenken.[189] Einerseits besteht die Gefahr eines „Übernahmeautomatismus" – sodass die Entscheidung letztendlich nicht durch den/die Richter*in gefällt wird, sondern nur noch verkündet.[190] Befürchtet wird, dass ein hohes Vertrauen in die „Unfehlbarkeit" der KI gesetzt wird. Erste Beispiele, wie die in einigen US-Bundesstaaten eingesetzte Software im Bereich der Strafzumessung, deuten allerdings auf die Gefahr der Verfestigung systematischer Diskriminierung, welche sich bei flächendeckendem Einsatz von KI-Programmen besonders ausweiten würde.[191] Ein wesentliches Merkmal des Rechtsanwendungsprozesses und damit auch einem „fairen Verfahren" ist zudem das fortlaufende Hinterfragen von Rechtsständen und Feststellen von Reformbedarfen und Neubewertungen.[192]

3.1.4.2 Gruppenspezifische Rechte

Recht der Arbeitnehmer auf gerechte und angemessene Arbeitsbedingungen (Art. 31): Die Regelung wird überwiegend nicht als ein allgemeines Recht auf „gerechte" Arbeitsbedingungen verstanden, sondern gewährt Beschäftigten ein einklagbares, subjektives Recht auf den Schutz von Körper und Gesundheit (physische und psychische Integrität) sowie ihrer Würde als Person im Beschäftigungsverhältnis.[193]

> (1) Jede Arbeitnehmerin und jeder Arbeitnehmer hat das Recht auf gesunde, sichere und würdige Arbeitsbedingungen.

Es gilt der unionsrechtliche Arbeitnehmerbegriff, wonach alle natürlichen Personen als Arbeitnehmer*in zählen, der:die Arbeit für eine bestimmte Zeit auf Weisung und gegen Entgelt verrichtet.[194] Unter „Arbeitsbedingen" lassen sich folgende Punkte verorten:

- *Arbeitsumfeld, Räumlichkeit und Ausstattung:* Einrichtung und Gestaltung der Arbeitsstätte und des Arbeitsplatzes; Gestaltung, Auswahl und Einsatz von Arbeitsmitteln;
- *Leistungsmodalitäten:* Gestaltung von Arbeitsverfahren und -abläufen und deren Zusammenwirken; Verteilung von Arbeitsaufträgen, Arbeitsrhythmus und Personalverteilung; Stand von Ausbildung und Unterweisung;
- *Betriebsbedingte Gefahren, Risiko- und Unfallfaktoren:* Verhütung von Berufsunfällen und Berufskrankheiten sowie der Gesundheitsschutz; Art, Grad und Dauer der physikalischen, chemischen und biologischen Einwirkungen.[195]

Im Hinblick auf menschengerechte, würdige und nicht-diskriminierende Arbeitsbedingungen werden vielfache Gefahren beim Einsatz von KI-Systemen gesehen. Sofern der KI-Einsatz bei der (Vor-)Auswertung von Be-

[188] *Stein, vom*, NZA 2021, 1057 (1060).
[189] *Enders*, JA 2018, 721 (723).; a.A. Beschluss der Justizministerkonferenz Beschluss zu TOP 1.11 (Nr. 2), abrufbar unter https://www.justiz.nrw.de/JM/jumiko/beschluesse/2019/Fruehjahrskonferenz_2019/I-11_Legal_Tech.pdf [letzter Abruf am 01.07.2022] sofern es sich um bloße *Unterstützung* handelt.
[190] *Enders*, JA 2018, 721 (723).
[191] Vgl. *Steinrötter/Warmuth,* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht Teil 30 Legal Tech Rn. 61 m.w.N., Rn. 68.
[192] *Steinrötter/Warmuth,* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht Teil 30 Legal Tech Rn. 70.
[193] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 31 Rn. 2; *Schubert,* in: EuArbRK Art. 31 GRC Rn. 1; *Krebber,* in: Callies/Ruffert, EUV/AEUV Art. 31 Rn. 2.
[194] *Schubert,* in: EuArbRK Art. 31 GRC Rn. 8; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 31 Rn. 6.
[195] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 31 Rn. 7; *Schubert,* in: EuArbRK Art. 31 GRC Rn. 11.

werbungen vermeintlich objektive, in Wirklichkeit aber „voreingenommene“ Kriterien ansetzt, kann das Allgemeine Gleichbehandlungsgesetz Schutzwirkung entfalten, welches u.a. Rechte der Beschäftigten auf einfach-rechtlicher Ebene umsetzt.[196] Rechtliche Implikationen stellen sich auch, wenn Software etwa eine Sozialauswahl bei Kündigungen gemäß § 1 Abs. 1 KSchG automatisiert vornimmt.[197]

Verbraucherschutz (Art. 38): Die EU will das Konzept der informierten Verbraucher*in sicherstellen, um sie vor Schäden zu schützen und eine vernünftige Ausübung ihrer Rolle zu ermöglichen.[198]

> Die Politik der Union stellt ein hohes Verbraucherschutzniveau sicher.

Die Regelung enthält allerdings nur einen Grundsatz und kein einklagbares Recht.[199] Verbraucherrechte sind tangiert, wenn KI bspw. im Rahmen der Vertragsgestaltung zum Einsatz kommt.[200]

Rechte des Kindes (Art. 24): Die Regelung umfasst sowohl den Schutz des kindlichen Wohlergehens und der Eltern-Kind-Beziehung und verleiht nach überwiegender Meinung Kindern als Rechtssubjekte eigenständige Leistungs- und Abwehrrechte.[201] Die Norm verbindet Teilhabe- und Schutzansprüche: im Rahmen ihrer Zuständigkeiten sind Union und Mitgliedstaaten dazu verpflichtet, alle Maßnahmen stets auch im Hinblick auf ihre Auswirkungen auf Kinder zu überprüfen sowie aktiv (schützend) für das Wohlergehen des Kindes einzutreten.[202] Dies gilt auch für die Regulierung von KI-Systemen.

Integration von Menschen mit Behinderung (Art. 26): Gerade die Gefahr einer Manifestation und Verfestigung von Diskriminierung durch das Einlernen historischer Daten und automatisierte Reproduzieren auch von Fehlentscheidungen begründet die Besorgnis einer Schlechterstellung von Menschen mit Behinderung.

> Die Union anerkennt und achtet den Anspruch von Menschen mit Behinderung auf Maßnahmen zur Gewährleistung ihrer Eigenständigkeit, ihrer sozialen und beruflichen Eingliederung und ihrer Teilnahme am Leben der Gemeinschaft.

Die Gewährleistung enthält allerdings einen bloßen Grundsatz i.S.d. Art. 52 Abs. 5 EU-GrCh, der durch Bestimmungen des Unionsrechts oder des nationalen Rechts konkretisiert werden muss.[203] Der Artikel selbst kann für sich allein dem Einzelnen kein subjektives Recht verleihen, das als solches geltend gemacht werden kann.[204]

Recht auf ein hohes Umweltschutzniveau und Verbesserung der Umweltqualität (Art. 37): auch in Bezug auf die Gesundheit und Sicherheit von Menschen.

> Ein hohes Umweltschutzniveau und die Verbesserung der Umweltqualität müssen in die Politik der Union einbezogen und nach

[196] *Enders*, JA 2018, 721 (722); *Dzida/Groh*, NJW 2018, 1917.
[197] *Stein, vom*, NZA 2021, 1057 (1060).
[198] Vgl. *Jarass*, Charta der Grundrechte der Europäischen Union Art. 38 Rn. 1 ff.
[199] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 38 Rn. 3.
[200] Siehe hierzu: *Grapentin*, NJW 2019, 181 (183).
[201] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 24 Rn. 3 f. m.w.N. *Hölscheidt,* in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union Art. 24 Rn. 17; *Kingreen,* in: Callies/Ruffert, EUV/AEUV Art. 24 Rn. 3.
[202] *Kingreen,* in: Callies/Ruffert, EUV/AEUV Art. 24 Rn. 3.
[203] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 26 Rn. 3.; EuGH, Urteil vom 22.05.2014 – C-356/12 – Glatzel, Rn. 78.
[204] EuGH, Urteil vom 22.05.2014 – C-356/12 – Glatzel, Rn. 78.

dem Grundsatz der nachhaltigen Entwicklung sichergestellt werden.

Auch hierbei handelt es sich lediglich um einen Grundsatz und kein einklagbares, subjektives Recht – dies folgt bereits aus der Unbestimmtheit und unklaren Zuordnung eines Grundrechtsträgers.[205] Allerdings können im Rahmen der Inzidenzkontrolle die Vereinbarkeit von Rechtsvorschriften mit dem Grundsatz überprüft werden und die Regelung kann so insgesamt eine umweltfreundliche Auslegung des EU-Rechts fördern.[206]

3.2 Grundrechte als Abwehrrechte gegenüber staatlichen Stellen

Setzten staatliche Akteure KI-Systeme ein, welche einen Eingriff in ein Grundrecht bewirken, können Betroffene die Grundrechte direkt als Abwehrrechte gegenüber diesem staatlichen Eingriff geltend machen. Dieser hat seine Handlungen gegenüber den Betroffenen zu rechtfertigen. Gleichzeitig vermitteln Grundrechte auch Teilhabe- und Schutzpflichten. So treffen den Staat Handlungspflichten, die Grundrechtspositionen seiner Bürger*innen vor Gefährdungen Dritter angemessen zu schützen, bspw. über eine regulierende Gesetzgebung sowie Etablierung von Durchsetzungs- und Kontrollmechanismen.

3.3 Reichweite des Grundrechtsschutzes im Privatrechtsverhältnis und Grundrechtskollision

Die mittelbare Drittwirkung der Grundrechte bedeutet, dass der Staat betroffene Personen im Verhältnis gegenüber Gefährdungen durch andere Private in ihrer Grundrechtsausübung schützen muss.[207] In Bezug auf das Verhältnis von Beschäftigten zu Arbeitgeber*innen bedeutet dies folgendes: Sofern es zu privatrechtlichen Streitigkeiten zwischen diesen beiden Parteien kommt, muss die Judikative den Schutzgehalt des Grundrechts beachten, wenn sie nicht das Grundrecht der Bürger*innen in seiner Funktion als Schutznorm verletzen will.[208] Folglich haben die Grundrechte eine entscheidende Bedeutung bei der Anwendung und Auslegung des einfachen Rechts.

Da sowohl die vom Einsatz eines KI-Systems betroffene Personen als auch die dieses einsetzende Stellen sich jeweils auf Grundrechtsschutz berufen können, muss eine Abwägung getroffen werden, welche sich oftmals bereits in der Ausgestaltung des einfachen Rechts wiederfindet. Enthalten die direkt anzuwendenden Normen Auslegungsspielräume oder Abwägungsklauseln, kommt es mittelbar zum Rückgriff auf die widerstreitenden Grundrechte.

Sämtliche Grundrechte der EU-Grundrechtecharta unterstehen der allgemeinen Schrankenregelung des Art. 52 Abs. 1 EU-GrCh. Grundrechtseingriffe müssen stets den Wesensgehalt der Rechte und Freiheiten achten.[209] Einschränkungen aufgrund des Schutzes der Rechte und Freiheiten anderer Personen bedürfen stets

[205] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 37 Rn. 3.
[206] *Jarass*, Charta der Grundrechte der Europäischen Union Art. 37 Rn. 3.
[207] Vgl. BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn. 30, WM 2006, 2270 ff.
[208] Vgl. BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn. 30, WM 2006, 2270 ff.
[209] Im Rahmen der Vorratsdatenspeicherung sah der EuGH den Wesensgehalt noch nicht verletzt, da sich die erfassten Daten nicht auf den Inhalt der Kommunikation bezogen: EuGH, Urteil vom 8.04.2014, C-293/12 und C-594/12 - Digital Rights Ireland, Rn. 39.

der Wahrung des Grundsatzes der Verhältnismäßigkeit.[210] Bewertungskriterien für eine Angemessenheitsprüfung können zunächst die Folgewirkungen auf andere Freiheitsrechte sein.[211] Den Gerichten kommt die Aufgabe zu, auf Basis des einschlägigen Fachrechts die jeweils entgegenstehenden Grundrechte der unterschiedlichen Seiten in Ausgleich zu bringen.[212]

Ähnliche Weichenstellungen gebietet das Grundgesetz: Eingriffe in das Recht auf informationelle Selbstbestimmung müssen im Rahmen der sog. „praktischen Konkordanz" mit konfligierenden Gegenpositionen abgewogen werden und dabei einen legitimen Zweck verfolgen, zur Erreichung des Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein.[213] Grundrechteingriffe sind „Erforderlich", wenn andere Maßnahmen mit geringerem Eingriffsgewicht diesen Zweck nicht vergleichbar effektiv erreichen.[214] Sie sind „Verhältnismäßig im engeren Sinne", wenn der mit ihnen verfolgte Zweck zu dem in ihnen liegenden Eingriffsgewicht nicht außer Verhältnis steht.

[210] Da jede Grundrechtseinschränkung gesetzlich vorgesehen sein muss, hat dies zur Folge, dass die gesetzliche Grundlage für den Eingriff den Umfang der Einschränkung selbst festlegen muss. EuGH, Urteil vom 8.04.2014, C-293/12 und C-594/12 - Digital Rights Ireland, Rn. 38; EuGH, Gutachten vom 26.07.2017 – 1/15 –, Rn. 138; EuGH, Urteil vom 17.12.2015 – C-419/14 – WebMindLicenses, Rn. 81; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 13ff.

[211] *Britz*, EuGRZ 2009, 1 (10) mit Verweis auf EuGH, Urteil vom 20.05.2003, C-465/00 – ORF (Österreichischer Rundfunk), Rn. 89.

[212] BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II, Rn. 96.

[213] BVerfGE 150, 244 (279) – Kfz-Kennzeichenkontrollen Bayern.

[214] BVerfGE 150, 244 (280), Rn. 88 – Kfz-Kennzeichenkontrollen Bayern.

4 Anwendbares Datenschutzrecht

Datenschutzrechtliche Anforderungen erwachsen nur, wenn das Datenschutzrecht auf den Sachverhalt anwendbar ist. Dabei gilt zu berücksichtigen, welches konkrete Regelungswerk sachlich und räumlich einschlägig ist.

Recht der Europäischen Union:

- **Datenschutz-Grundverordnung – DSGVO:** Zentrales Instrument zum Schutz personenbezogener Daten in der EU, welche als unmittelbar anwendbare Verordnung Rechte und Pflichten statuiert, allerdings auch zahlreiche Öffnungsklauseln enthält, die weiterhin in begrenztem Umfang mitgliedstaatliche Regelungen ermöglichen.
- **ePrivacy-Richtlinie:** Bereichsspezifische Datenschutzregeln für die Telekommunikation und Telemedien, als Richtlinie allerdings nicht unmittelbar anwendbar, sondern muss durch mitgliedstaatliches Recht umgesetzt werden, welches richtlinienkonform auszulegen ist.
- **JI-Richtlinie:** Datenschutz-Richtlinie im Bereich von Justiz und Inneres

Recht Deutschland:

Bundesebene

- **Bundesdatenschutzgesetz – BDSG:** füllt die Öffnungsklauseln der DSGVO konkretisierend aus und setzt die JI-Richtlinie um.
- **Telekommunikation-Telemedien-Datenschutzgesetz – TTDSG:** Umsetzung der ePrivacy-Richtlinie (vormals Telekommunikationsgesetz - TKG und Telemediengesetz - TMG)

Landesebene

- Landesdatenschutzgesetze: Baden-Württemberg **LDSG BW**, Bayern **BayDSG**, Berlin **BlnDSG**, Brandenburg **BbgDSG**, Bremen **BremDSGVOAG**, Hamburg **HmbDSG**, Hessen **HDSIG**, Mecklenburg-Vorpommern **DSG M-V**, Niedersachsen **NDSG**, Nordrhein-Westfalen **DSG NRW**, Rheinland-Pfalz **LDSG RhPfl**, Saarland **SaarlDSG**, Sachsen **SächsDSG**, Sachsen-Anhalt **DSG LSA**, Schleswig-Holstein **LDSG SH**, Thüringen **ThürDSG**

Exemplarische Beispiele für sektorspezifisches Recht mit Bezug zum Datenschutz:

Gesundheit

- **SGB V** elektronische Gesundheitskarte (eGK), Datenverarbeitung durch Krankenkassen, Forschungsdatenzentrum (§ 303d SGB V)
- **Krankenhausgesetze**

Mobilität

- **General Safety Regulation:** Art. 6 Abs. 4 VO (EU) 2019/2144 zum Umfalldatenspeicher
- **Straßenverkehrsgesetz:** § 1g, §§ 63a, 63b StVG zum Fahrmodusspeicher
- **Mobilitätsdatenverordnung:** Zugang zu Daten aus dem Bereich Personenbeförderung

Energie

- **Messstellenbetriebsgesetz – MsbG**: Datenschutz- und Datensicherheitsanforderungen an Messsysteme

Bildung

- **Landeshochschulgesetze** Datenverarbeitung zur Erfüllung der Aufgaben einer Hochschule
- **Landesschulgesetze**

Kirchenrecht

- **Gesetz über den kirchlichen Datenschutz – KDG**: der katholischen Kirche.
- **Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland - DSG-EKD**

4.1 Anwendbarkeit der DSGVO

Zur Ermittlung der rechtlichen Anforderungen an eine geplante Datenverarbeitung ist im ersten Schritt zu prüfen, ob der Anwendungsbereich der DSGVO eröffnet ist. Der sachliche und räumliche Anwendungsbereich der DSGVO werden in Art. 2 und 3 DSGVO normiert.

4.1.1 Sachliche Anwendbarkeit

Art. 2 Abs. 1 DSGVO nennt die grundlegenden Voraussetzungen, die erfüllt sein müssen, damit die DSGVO zur Anwendung kommt. Dies sind:

Abbildung 6 zum sachlichen Anwendungsbereich

4.1.1.1 Ganz oder teilweise automatisierte Verarbeitung

Weiterhin müssen personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden, damit der Anwendungsbereich der DSGVO eröffnet ist. Der Begriff der „Verarbeitung“ wird definiert als:

> **Art. 4 Nr. 2 DSGVO** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten 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 eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Aus dieser Definition ist zu erkennen, dass der Begriff sehr weit auszulegen ist und letztlich jede Form von Datenverarbeitungstätigkeiten umfasst.[215] Dies gilt auch für flüchtige Verarbeitungen.[216] Ebenso gilt zu bedenken, dass auch eine Anonymisierung unter den Verarbeitungsbegriff subsumiert wird.[217] Folglich sind die Grundsätze der DSGVO zunächst auch dann zu beachten, wenn beabsichtigt wird, Daten anonym zu verarbeiten, sofern dies erst über eine Durchzuführende Anonymisierung möglich wird.

Die Differenzierung zwischen einer ganz oder teilweise automatisierten Verarbeitung erfolgt über mögliche händische Zwischenschritte. Eine Teilautomatisierung liegt etwa vor, wenn personenbezogene Daten manuell in eine digitale Datenbank eingegeben werden.[218]

[215] *Kühling/Raab,* in: Kühling/Buchner, DS-GVO Art. 2 Rn. 15; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 2 Rn. 5; *Roßnagel,* in: NK Datenschutzrecht Art. 2 Rn. 14.
[216] Vgl. insoweit die geänderte Sichtweise des BVerfG zur Rechtfertigungsbedürftigkeit: BVerfGE 150, 309 (330), Rn. 54 – Kfz-Kennzeichenkontrollen BW-HE; BVerfGE 150, 244-309, Rn. 39 – Kfz-Kennzeichenkontrollen Bayern.
[217] *BfDI*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 5; *Roßnagel,* in: NK Datenschutzrecht Art. 4 Nr. 2 Rn. 12; *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 23.
[218] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 3.

4.1.1.2 Nicht automatisierte Verarbeitung

Auch die nichtautomatisierte Verarbeitung personenbezogener Daten unterfällt dem sachlichen Anwendungsbereich der DSGVO, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Schutz natürlicher Personen soll technologieneutral sein und daher neben der automatisierten gleichermaßen auch die manuelle Verarbeitung von personenbezogenen Daten umfassen (vgl. ErwGr. 15).[219]

> **Art. 4 Nr. 6 DSGVO** „Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird

Somit werden grundsätzlich auch alle geordneten manuellen Datenverarbeitungen erfasst, sodass selbst handschriftliche Notizen unter den Anwendungsbereich fallen, sofern diese nach gewissen strukturierenden Kriterien geordnet werden.[220]

4.1.1.3 Ausnahmen

Art. 2 Abs. 2 DSGVO nennt Ausnahmen vom Anwendungsbereich, bei deren Vorliegen die DSGVO trotz Erfüllung der in Art. 2 Abs. 1 DSGVO genannten Voraussetzungen dennoch keine Anwendung findet.

Haushaltsausnahme: Einen wesentlichen Unterschied macht es, ob KI-Systeme privat im Familien- und Freundeskreis oder im beruflichen Kontext eingesetzt werden. Denn die DSGVO nimmt reine Privatkontexte vom Anwendungsbereich aus. Dies ist dann der Fall, wenn die Datenverarbeitung durch eine natürliche Person „ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird" (ErwGr. 18 S. 1 DSGVO). Diese sog. Haushaltsausnahme beruht auf dem Gedanken, dass eine übermäßige Regulierung die freie Entfaltung der Persönlichkeit gefährden könnte und dient somit dem Schutz der Privatsphäre.[221] Dies führt zu unterschiedlichen Konsequenzen bei der Verwendung von IT-Lösungen im privaten und im dienstlichen Kontext.[222]

Strafverfolgung: In Abgrenzung zur JI-RL wird die hoheitliche Kriminalitätsbekämpfung vom Anwendungsbereich der DSGVO ausgenommen.

Tätigkeiten außerhalb des Anwendungsbereichs des Unionsrechts: Datenverarbeitungen durch Private fallen in die EU-Regelungskompetenz zum freien Datenverkehr, sodass die Ausnahme nur bei staatlicher Datenverarbeitung greift, die vom Anwendungsbereich des Unionsrechts nicht mehr erfasst ist.[223] Darunter fallen Tätigkeiten im Rahmen der Sicherstellung der nationalen Sicherheit sowie Tätigkeiten, die derselben Kategorie zugeordnet werden können.[224]

Gemeinsame Außen- und Sicherheitspolitik: Auch diese Ausnahme zeichnet die EU-Regelungskompetenz nach.[225]

---

[219] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 2 Rn. 5.
[220] EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 57.
[221] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 12; *Kühling/Raab,* in: Kühling/Buchner - DS-GVO/BDSG Art. 2 Rn. 10; *Gola/Lepperhoff*, ZD 2016, 9 (11).
[222] Eine Datenverarbeitung, die auch – aber nicht nur – persönlichen Zwecken dient, dürfte dabei nicht privilegiert sein: *Piltz*, K&R 2016, 557 (558).
[223] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 8.
[224] EuGH, Urteil vom 22.06.2021 –C-439/19, Rn. 66.
[225] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 10.

4.1.2 Räumliche Anwendbarkeit der DSGVO

Art. 3 DSGVO bestimmt die räumliche Anwendbarkeit der DSGVO und ist in drei Absätze aufgeteilt. Dabei sind zwei wesentliche Prinzipien zu unterscheiden: Sitzlandprinzip (Abs. 1) und das Marktortprinzip (Abs. 2).[226]

Sitzlandprinzip	Marktortprinzip	Rechtliche Exklave
Verantwortlicher / Auftragsverarbeiter haben Niederlassung in EU, unabhängig wo Verarbeitung stattfindet	Angebot von Waren/Diensten an Betroffene innerhalb der Union oder Beobachtung ihres Verhaltens	Ort, an dem das Recht eines Mitgliedstaats aufgrund des Völkerrechts gilt

4.1.2.1 Sitzlandprinzip

Art. 3 Abs. 1 betrifft Sachverhalte, in denen sich die Niederlassung in der Union befindet, die an der Datenverarbeitung beteiligt ist. Das Sitzlandprinzip schreibt die Regelung aus der Datenschutzrichtlinie in Art. 4 Abs. 1 Buchst. a RL 95/46/EG fort.[227] Demzufolge findet die DSGVO auf die Verarbeitung personenbezogener Daten Anwendung, soweit diese seitens eines Verantwortlichen oder Auftragsverarbeiters im Rahmen der Tätigkeit einer Niederlassung in der EU erfolgt. Dabei muss sich die datenverarbeitende Hardware nicht in der Union befinden.[228] Diese Entkopplung zwischen Sitz der Niederlassung und tatsächlichem Ort der Datenverarbeitung ist der zunehmend globalen und vernetzten Verarbeitung der Daten, bspw. in der Cloud, geschuldet. [229] Folglich ist es unerheblich, ob die Verarbeitung selbst in der EU stattfindet. Erfolgt die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer in der EU verorteten Niederlassung, ist die DSGVO bereits anwendbar.[230] Sofern das Unternehmen, in dessen (Mit-)Verantwortung die Datenverarbeitung liegt, seinen Sitz innerhalb der EU hat, ist die DSGVO aufgrund des Sitzlandprinzips anwendbar.

4.1.2.2 Marktortprinzip

Die DSGVO erweitert ihren räumlichen Anwendungsbereich auf nicht in der EU niedergelassene Stellen, wenn diese Waren oder Dienstleistungen unentgeltlich oder entgeltlich an betroffene Personen anbieten oder das Verhalten betroffener Person beobachten, auch wenn der Verantwortliche oder Auftragsverarbeiter

[226] *Piltz,* in: Gola DS-GVO, Art. 3 Rn. 5.
[227] *Piltz*, K&R 2016, 557 (558).
[228] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG Art. 3 Rn. 7. Eine Niederlassung kann bspw. bereits bei Vorhandensein einer Vertretung und eines Bankkontos in einem Mitgliedstaat gegeben sein: *Piltz*, K&R 2016, 557 (558); *Mausbach*, ZD 2019, 450 (451).
[229] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG Art. 3 Rn. 7.
[230] EuGH, Urt. v. 28.7.2016 – C-191/15 – Verein für Konsumenteninformation, Rn. 74; *Piltz,* in: Gola DS-GVO, Art. 3 Rn. 8.

keine (relevante) Niederlassung in der Union hat (Marktortprinzip).[231] Die betroffenen Personen, deren Daten verarbeitet werden, müssen sich (zumindest vorübergehend) im Unionsgebiet aufhalten, wobei ein (fester) Wohnsitz oder die Unionsbürgerschaft dagegen keine Voraussetzung sind.[232] Mit dem Marktortprinzip wird sichergestellt, dass auch die verantwortlichen Unternehmen, die sich zwar nicht in der Union niedergelassen haben, aber dennoch aktiv in datenschutzrechtlich relevanter Weise am europäischen Binnenmarkt teilnehmen, an die Anforderungen der DSGVO gebunden sind.[233]

Art. 3 Abs. 2 DSGVO

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

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

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

Absatz 3 erstreckt den Anwendungsbereich der DSGVO zudem auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt. Dies bezieht sich insbesondere auf die diplomatischen oder konsularischen Vertretungen eines Mitgliedstaates im Ausland außerhalb der EU.[234]

4.2 Anwendbarkeit des BDSG

Neben bzw. ergänzend zu den Vorgaben der DSGVO können im hier betrachteten Kontext auch relevante Vorgaben aus dem mitgliedstaatlichen Recht – hier dem deutschen Recht – erwachsen. Insofern kommt es auch auf die sachliche und räumliche Anwendbarkeit des BDSG an. Die Rolle des BDSG hat sich mit der Einführung der DSGVO gewandelt, da die DSGVO als EU-Verordnung Anwendungsvorrang genießt und damit das bisherige BDSG a.F. weitgehend verdrängt hätte. Die Aufgabe des novellierten BDSG liegt nun zum einen in der Ausfüllung von Öffnungs- und Konkretisierungsklauseln der DSGVO und zum anderen der Umsetzung der JI-Richtlinie.

4.2.1 Sachlicher und persönlicher Anwendungsbereich

Das BDSG gilt gemäß §1 Abs. 1 S. 1 Nr. 1, 2 und S. 2 BDSG für die Verarbeitung personenbezogener Daten durch:

- öffentliche Stellen des Bundes,
- öffentliche Stellen der Länder, in bestimmten Fällen sofern nicht ein Landesgesetz den Datenschutz bereits regelt,

[231] Zu Auslegungsschwierigkeiten bei Anwendung des Marktotprinzips, wenn eine Niederlassung in der Union existiert, das Sitzlandprinzip aber nicht greift: *Piltz*, K&R 2016, 557 (559). Zur Auslegung des „Beobachtens“: *Mausbach*, ZD 2019, 450 (451).
[232] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 3 Rn. 8; *Zerdick,* in: Ehmann/Selmayr - DSGVO Art. 3 Rn. 17.
[233] *Ennöckel,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 3 Rn. 12; *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG Art. 3 Rn. 16; *Piltz*, K&R 2016, 557 (558).
[234] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 3 Rn. 21.

- sonstige Adressaten (nichtöffentliche Stellen), unter denselben Voraussetzungen, die der sachlichen Anwendbarkeit der DSGVO entsprechen.

Öffentlich Stellen sind Stellen, die öffentlich-rechtliche Aufgaben wahrnehmen.[235] Hier gilt das BDSG für sämtliche Formen der Verarbeitung personenbezogener Daten und ist somit weiter als die DSGVO.[236] Für die sonstigen nichtöffentlichen Stellen entspricht die Formulierung des sachlichen Anwendungsbereichs hingegen bewusst der des Art. 2 Abs. 1 Buchst. c DSGVO (inkl. Haushaltsausnahme in Art. 2 Abs. 2 DSGVO), um die sachliche Anwendung des BDSG im Rahmen der Öffnungsklauseln inhaltsgleich zur Anwendung der DSGVO zu gestalten.[237] Darüber hinaus gilt das BDSG nach § 26 Abs. 7 BDSG in Beschäftigungsverhältnissen auch für die nicht dateimäßige Verarbeitung personenbezogener Daten (siehe Abschnitt 8).[238]

4.2.2 Räumlicher Anwendungsbereich

Bezüglich der Anwendbarkeit auf öffentliche Stellen bedarf es keiner spezifischen Regelungen zum territorialen Anwendungsbereich (vgl. § 1 Abs. 4 S. 1 BDSG). Für die nichtöffentlichen Stellen gibt § 1 Abs. 4 S. 2 Nr. 1-3 BDSG Auskunft über die Reichweite der räumlichen Anwendbarkeit:

- der Verantwortliche oder Auftragsverarbeiter verarbeitet personenbezogene Daten im Inland,
- die Datenverarbeitung erfolgt im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters oder
- die Verarbeitung erfolgt im Anwendungsbereich der DSGVO.

Die erste Alternative knüpft an die Belegenheit der IT-Infrastruktur an.[239] Diese steht in gewissem Widerspruch zur DSGVO, welche an die Niederlassung anknüpft und den Ort der Datenverarbeitung selbst bewusst unberücksichtigt lässt.[240] Das BDSG könnte folglich auch in Fällen zur Anwendung kommen, in denen die DSGVO nicht anwendbar ist.[241] Die zweite Alternative entspricht dem Sitzlandprinzip der DSGVO.[242] Die letzte Alternative ist als Verweis auf das Marktortprinzip zu verstehen, d.h. das BDSG kommt auch in Fällen zur Anwendung, in denen zwar keine Niederlassung im Inland besteht, die DSGVO nichtsdestotrotz über Art. 3 Abs. 2 DSGVO anwendbar ist.[243] Im Wege der einschränkenden Auslegung wird angeraten, das BDSG entgegen des als zu weit geraten kritisierten Wortlauts nicht in Fällen anzuwenden, in denen lediglich Bezug zu einem anderen EU-Staat besteht.[244] Sind die genannten Alternativen nicht einschlägig, so gelten nach § 1 Abs. 4 S. 3 BDSG nichtsdestotrotz die Regelungen zu den Aufsichtsbehörden, Sanktionen und Rechtsbehelfen in den §§ 8-21, 39 und 44 BDSG.[245]

---

[235] *Gusy/Eichenhofer,* in: BeckOK DatenschutzR, § 1 Rn. 73; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 4.
[236] *Ernst,* in: Paal/Pauly, DS-GVO, § 1 Rn. 2; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 5.
[237] BT-Drs. 18/11325, S. 79; *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 12.
[238] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 13.
[239] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 29; *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 22 ff.
[240] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 23; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 18.
[241] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 24. Da diese Frage außerhalb des Anwendungsbereichs der DSGVO liegt, besteht kein Grund für die Annahme der Europarechtswidrigkeit (str. vgl. *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 30.).
[242] *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 17.
[243] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 29; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 19; *Ernst,* in: Paal/Pauly - DS-GVO BDSG, § 1 Rn. 12; *Gusy/Eichenhofer,* in: BeckOK DatenschutzR, § 1 Rn. 101c.
[244] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 34; *Ernst,* in: Paal/Pauly - DS-GVO BDSG, § 1 Rn. 12.
[245] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 19; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 17.

4.2.3 Grundsatz der Subsidiarität

Gemäß § 1 Abs. 2 S. 1 BDSG gehen andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG vor. Das BDSG findet nur insoweit Anwendung, wie die vorrangige Spezialregelung einen Sachverhalt nicht oder nicht abschließend regelt (§ 1 Abs. 2 S. 2 BDSG). In Fällen der Tatbestandskongruenz gehen somit speziellere Regelungen dem BDSG vor, sofern der Regelungsgegenstand deckungsgleich ist.[246] Das BDSG hat folglich den Charakter eines Auffanggesetzes.[247] Es kommt nur zur Anwendung, wenn keine spezifischere Regelung besteht oder diese nicht abschließend ist. Im vorliegenden Unternehmenskontext relevante Spezialregelungen finden sich bspw. in der Abgabenordnung (AO), im Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) oder Kreditwesengesetz (KWG). § 1 Abs. 5 BDSG weist auf den aus Art. 288 Abs. 2 AEUV folgenden Anwendungsvorrang des EU-Rechts hin. Dieser Absatz hat lediglich klarstellende Funktion.[248]

4.3 Anwendbarkeit des Landesdatenschutzrechts

Die Landesdatenschutzgesetze gelten regelmäßig nur für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des jeweiligen Landes.[249] Hierbei handelt es sich zumeist um Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (vgl. § 2 Abs. 1 S. 1 LDSG BW). § 2 Abs. 2 LDSG BW weitetet den Anwendungsbereich in Baden-Württemberg auch auf juristische Personen und sonstige Vereinigungen des privaten Rechts aus, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in § 2 Abs. 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Im Kontext der KI-Forschung ist zu berücksichtigen, dass Hochschulen unter das jeweilige Landesrecht fallen.

4.4 Zwischenergebnis zum anwendbaren Recht

Die Grundlegenden Weichenstellungen zur Anwendbarkeit des Datenschutzrechts setzt die DSGVO. Hierbei ist im Wesentlichen zu klären:

- Werden **personenbezogene Daten** verarbeitet?
  - Im Hinblick auf KI-Systeme sind sowohl die Trainings- und Eingabedaten als auch die Entscheidungsergebnisse in den Blick zu nehmen.
  - Bei Anonymisierung ist zu klären, ob Daten hinreichend anonym sind und wie (Re-) Identifizierungsrisiken zu bewerten sind.
- Wer ist der für die Verarbeitung **Verantwortliche:** hat dieser seinen Sitz in der EU (Sitzlandprinzip) oder greift das Marktortprinzip?

Dem BDSG kommt insbesondere bei der Verarbeitung personenbezogener Daten im Beschäftigtenverhältnis Bedeutung zu, da die DSGVO insoweit in Art. 88 DSGVO eine Öffnungsklausel für Konkretisierungen im mitgliedstaatlichen Recht bereit hält.

---

[246] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 16; *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 15.
[247] *Ernst,* in: Paal/Pauly - DS-GVO BDSG, § 1 Rn. 6 ff.; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 11; *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 14.
[248] BT-Drs. 18/11325, S. 80.
[249] Siehe bspw. § 2 Abs. 1 LDSG Baden-Württemberg.

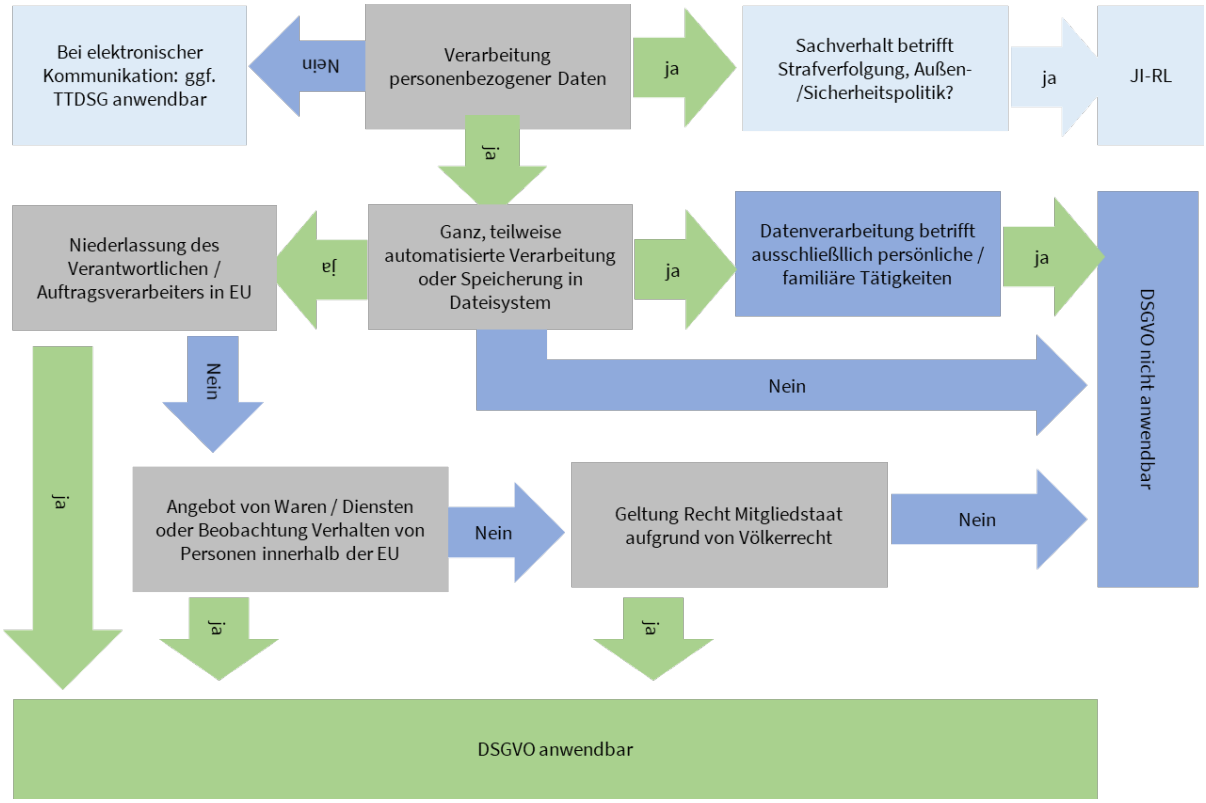


Abbildung 7 Prüfschema zur Anwendbarkeit der DSGVO

5 Datenschutzgrundprinzipien

Dem Datenschutzrecht liegen wesentliche Grundprinzipien zu Grunde.[250] Diese grundlegenden Datenschutzprinzipien werden in Art. 5 DSGVO festgehalten. Sie gelten für jede Datenverarbeitung unmittelbar, unabhängig davon, ob es sich beim jeweiligen Verantwortlichen oder Auftragsverarbeiter um eine private Stelle oder Träger hoheitlicher Gewalt handelt.[251] Verstöße gegen die Datenschutzgrundprinzipien des Art. 5 DSGVO können Sanktionen gemäß Art. 83 DSGVO nach sich ziehen (siehe Abschnitt 5.8.5).[252] Zudem werden die Prinzipien durch die Vorgaben der DSGVO sowie – im Rahmen der Öffnungsklauseln – durch das BDSG konkretisiert. Anhand der einzelnen Datenschutzprinzipien sollen im Folgenden der datenschutzrechtliche Pflichtenkanon erläutert werden.

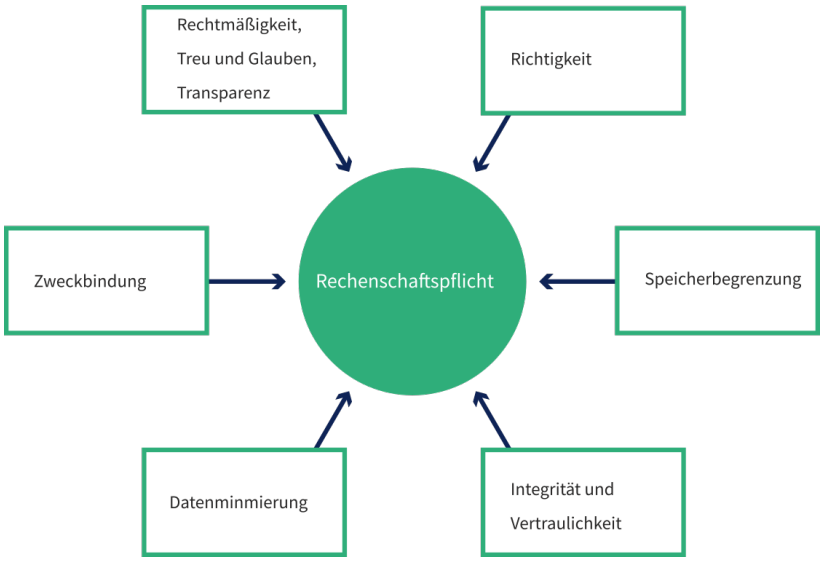


Abbildung 8 Die Datenschutzgrundprinzipien in Art. 5 DSGVO

5.1 Rechtmäßigkeit, Treu und Glauben

> **Art. 5 Abs. 1 Buchst. a DSGVO** Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

Das in Art. 5 Abs. 1 Buchst. a DSGVO kodifizierte Datenschutzprinzip besteht aus drei Teilbereichen: der *Rechtmäßigkeit*, der Verarbeitung nach *Treu und Glauben* und der Nachvollziehbarkeit bzw. *Transparenz*.[253] Die Rechtmäßigkeit der Verarbeitung wird in Art. 6 DSGVO konkretisierend geregelt (bzw. in Art. 9 DSGVO für besondere Kategorien personenbezogener Daten). Grundlage jeder Datenverarbeitung muss, folgt man der engeren Auslegung des Begriffs Rechtmäßigkeit,[254] eine der in Art. 6 Abs. 1 DSGVO genannten Legitimationsgrundlagen sein. Dies entspricht dem Prinzip des Verbots mit Erlaubnisvorbehalt, welches die Datenverarbei-

[250] Siehe für einen Überblick der Grundprinzipien in Bezug auf KI: *Gausling*, DSRITB 2018, 519 (529 ff.).
[251] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 5 Rn. 1.
[252] Zur Verbindlichkeit der Grundprinzipien: *Albrecht*, CR 2016, 88 (91); *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 2 m.w.N.
[253] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 5 Rn. 3.
[254] Zum wissenschaftlichen Streit: *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 5 Rn. 4 m.w.N.

tung, die im sachlichen und räumlichen Anwendungsbereich gemäß Art. 2, 3 DSGVO liegt, grundsätzlich verbietet, es sein denn, ein Erlaubnistatbestand liegt vor. Dies folgt auch aus der Tatsache, dass der EuGH bereits jegliche Form der Verarbeitung personenbezogener Daten als Eingriff in den Schutzbereich des Art. 8 Abs. 1 EU-GrCh wertet.[255] Die Notwendigkeit für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage heranziehen zu müssen, geht somit zurück auf die Datenschutzgrundrechte und wird im Rahmen der DSGVO durch den Grundsatz der Rechtsmäßigkeit in Art. 5 Abs. 1 Buchst. a sowie die Regelungen in Art. 6 Abs. 1 und Art. 9 Abs. 1, 2 DSGVO unterstrichen. Je nach Verarbeitungskontext kommen unterschiedliche Legitimationstatbestände in Betracht.

Der Grundsatz der Verarbeitung nach Treu und Glauben lässt sich besser mit Grundsatz der „Fairness" umschreiben.[256] Abgestellt werden kann auf die absehbare, vernünftige Erwartungshaltung der betroffenen Person, womit die Gewährleistung einer fairen Verarbeitung verbunden wäre.[257] Diesem Grundsatz kommt insbesondere bei Interessenabwägungen und im Rahmen von Verhältnismäßigkeitserwägungen eine Bedeutung zu.[258] Andere wiederum nennen den Grundsatz zuvörderst im Zusammenhang mit der Transparenz.[259] Erst die Möglichkeit eine Datenverarbeitung nachvollziehen und verstehen zu können, bildet einen Vertrauensanker für eine „faire" Verarbeitung.[260] Gerade die heimliche Datenverarbeitung wird als typischer Verstoß gegen den Fairnessgrundsatz genannt. [261] Der Grundsatz der Transparenz stellt daher Schnittmengen zum Grundsatz von Treu und Glauben dar und wird an vielen Stellen der DSGVO präzisiert. Dieser Grundsatz wird folgenden Abschnitt näher erläutert.

5.2 Transparenz

Transparenz dient der „Herstellung der Prüfbarkeit einer Verarbeitungstätigkeit".[262] Die Art. 12 bis 15 der DSGVO konkretisieren die Pflichten der Verantwortlichen hinsichtlich der Informationen, die vor oder bei der Verarbeitung der betroffenen Person zur Verfügung gestellt werden müssen. Das Prinzip der Transparenz ist über Art. 8 Abs. 2 EU-GrCh auch grundrechtlich verankert. Während Art. 13 f. DSGVO Informationspflichten *vor* der Datenverarbeitung adressieren, sind in Art. 15 DSGVO die Auskunftsrechte der Betroffenen normiert.[263]

---

[255] EuGH, Urteil vom 08. April 2014 – C-293/12 – Digital Rights Ireland, Rn. 36; EuGH, Urteil vom 17. Oktober 2013 – C-291/12 – Schwarz, Rn. 25; EuGH, Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 – Tele2 Sverige, Rn. 100; *Franzen,* in: Franzen/Gallner/Oetker, EuArbR Art. 8 GRC Rn. 7; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 8; *Gersdorf,* in: BeckOK InfoMedienR Art. 8 EU-GrCharta Rn. 18; *Bieker*, DuD 2018, 27 (28); *Roßnagel*, NJW 2019, 1 (2).

[256] *Schantz*, in: BeckOK DatenschutzR Art. 5 Rn. 7; *Herbst*, in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 14; *Frenzel*, in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 18; vgl. *Albrecht*, CR 2016, 88 (91).

[257] *Spindler/Dalby*, in: Recht der elektronischen Medien Art. 5 Rn. 5; *Schantz*, in: BeckOK DatenschutzR Art. 5 Rn. 8.

[258] *Spindler/Dalby*, in: Recht der elektronischen Medien Art. 5 Rn. 5.

[259] Im Hinblick auf den gleichlautenden Grundsatz im Rahmen der grundrechtlichen Verbürgung des Art. 8 EU-GrCh: *Purtova*, Property rights in personal data, S. 152; *Marsch*, Das europäische Datenschutzgrundrecht, S. 170 ff. vgl. zur Ableitung der Informationspflichten aus dem sekundärrechtlich verankerten Grundsatz von Treu und Glauben: EuGH, Urteil vom 01. Oktober 2015 – C-201/14 – Bara, Rn. 34.

[260] *Wagner,* Datenökonomie und Selbstdatenschutz, S. 234.

[261] *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 8; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 15; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 18; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 45; *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung Art. 5 Rn. 14.

[262] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 5.

[263] Umstritten ist, ob die Informationen zwingend vor oder spätestens gleichzeitig mit der Datenerhebung bereitzustellen sind: *Schmidt-Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 79; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 56; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 13 Rn. 12; *Knyrim,* in: Ehmann/Selmayr - DSGVO Art. 13 Rn. 10; *Franck,* in: Gola DS-GVO, Art. 13 Rn. 36.

5.2.1 Grundsatz

Im ErwGr. 39 werden die Grundsätze der Datenverarbeitung näher erläutert. Bestimmte Informationspflichten stellen danach die Basis für eine „faire und transparente Verarbeitung“ dar.[264]

> **ErwGr. 39 S. 2 – 5 DSGVO** Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.

Regelungen genereller Art sind in Art. 12 DSGVO enthalten, der u.a. verschiedene Modalitäten zur Bereitstellung der Informationen sowie Umsetzung der Rechte der betroffenen Personen normiert:

- Verantwortliche treffen „geeignete Maßnahmen“ zur Umsetzung der Informations-, Auskunfts- und sonstigen Betroffenenrechte.
- Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.
- Auskünfte sind auf Antrag „unverzüglich“ bereitzustellen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags (Verlängerungen um zwei Monate möglich, bei Komplexität / Anzahl der Anträge). Eine Reaktion muss in jedem Fall innerhalb eines Monats erfolgen.
- Antworten sollten elektronisch erfolgen, wenn die betroffene Person diesen Kommunikationsweg wählt.
- Auskünfte sind unentgeltlich bereitzustellen. Ausnahmen sind offenkundig unbegründete oder exzessive Anträge (hier darf ein angemessenes Entgelt berechnet oder Auskunft verweigert werden).
- Bei Zweifeln über die Identität des Antragstellenden dürfen weitere Informationen zur Identitätsbestätigung angefordert werden.
- Informationen dürfen in Kombination mit standardisierten Bildsymbolen bereitgestellt werden – sofern elektronisch, sollten diese maschinenlesbar sein.

Für die meisten KI-Analysen dürfte bezüglich der transparenten Darstellung die Herausforderung gerade darin bestehen, die Komplexität der eingesetzten analytischen Verfahren so zu beschreiben, dass deren Tragweite für die jeweils betroffenen Personen überhaupt greifbar ist.[265]

[264] Weitere Grundsätze, die in ErwGr. 39 erläutert werden betreffen die Beschränkung und Festlegung der Speicher- bzw. Löschfristen sowie die Berichtigungspflicht und die Sicherheit bzw. Vertraulichkeit der personenbezogenen Daten.

[265] *Gausling*, DSRITB 2018, 519 (529). Schlägt als Lösungsoption die Nutzung der gemäß Art. 42 DSGVO vorgesehenen datenschutzspezifischen Zertifizierungsverfahren und -prüfzeichen zum Nachweis der DSGVO-Compliance vor.

5.2.2 Informationspflichten

Konkrete Angaben der zu übermittelnden Informationen, dem Informationszeitpunkt und möglichen Ausnahmen sind in Art. 13 und 14 geregelt. Art. 13 DSGVO adressiert hierbei die Datenerhebung *bei der* betroffenen Person. Art. 14 DSGVO enthält hingegen Besonderheiten, wenn die Daten *nicht bei der* betroffenen Person selbst erhoben werden.

5.2.2.1 Datenerhebung bei der betroffenen Person

Adressat der Informationspflichten des Art. 13 DSGVO ist der Verantwortliche. Abs. 1 und 2 DSGVO legen diejenigen Informationen fest, die bereitgestellt werden müssen: diese werden in Tabelle 1 aufgelistet. Wenn eine Weiterverarbeitung zu einem anderen Zweck als den, für den die personenbezogenen Daten ursprünglich erhoben wurden, erfolgen soll, so hat der Verantwortliche nach Art. 13 Abs. 3 DSGVO der betroffenen Person vor dieser Weiterverarbeitung zusätzlich Informationen über diesen neuen Zweck und alle anderen maßgeblichen Informationen gemäß Abs. 2 zur Verfügung zu stellen.

5.2.2.2 Datenerhebung nicht bei der betroffenen Person

Art. 14 DSGVO regelt die Art und den Umfang der Informationspflicht des Verantwortlichen gegenüber der betroffenen Person, wenn und soweit die Daten nicht bei der betroffenen Person selbst erhoben werden. Die Abs. 1 und 2 entsprechen hierbei den Regelungen des Art. 13 Abs. 1 und 2 DSGVO (vgl. Tabelle 1 mit Hervorhebungen bei Abweichungen). Abs. 3 regelt, den spätesten Mitteilungszeitpunkt:

- Innerhalb einer „angemessenen Frist“ nach Erlangung der Daten, spätestens innerhalb eines Monats,
- Spätestens zum Zeitpunkt der ersten Kommunikationsaufnahme zur betroffenen Person,
- Bei Offenlegung an andere Empfänger: spätestens bei erster Offenlegung.

Art. 13 Abs. 1, 2 DSGVO	Art. 14 Abs. 1, 2 DSGVO
▪ Namen und Kontaktdaten des Verantwortlichen ▪ Ggf. Kontaktdaten Datenschutzbeauftragten ▪ Verarbeitungszwecke und Rechtsgrundlagen ▪ Im Fall der Interessenabwägung (Art. 6 Abs. 1 Buchst. f DSGVO): die berechtigten Interessen ▪ Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten ▪ Ggf. Absicht von Drittlandtransfers / Übermittlung an internationale Organisation, Vorhandensein / Fehlen Angemessenheitsbeschluss oder Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind ▪ Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer ▪ Auskunftsrecht, Recht auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit	▪ Namen und Kontaktdaten des Verantwortlichen ▪ Ggf. Kontaktdaten Datenschutzbeauftragten ▪ Verarbeitungszwecke und Rechtsgrundlagen ▪ Im Fall der Interessenabwägung (Art. 6 Abs. 1 Buchst. f DSGVO): die berechtigten Interessen ▪ Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten ▪ Ggf. Absicht von Drittlandtransfers / Übermittlung an internationale Organisation, Vorhandensein / Fehlen Angemessenheitsbeschluss oder Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind ▪ Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer ▪ Auskunftsrecht, Recht auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit

▪ Bei Einwilligung: Recht jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird ▪ Beschwerderecht bei einer Aufsichtsbehörde ▪ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person ▪ ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte	▪ Bei Einwilligung: Recht jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird ▪ Beschwerderecht bei einer Aufsichtsbehörde ▪ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person ▪ die Kategorien personenbezogener Daten, die verarbeitet werden ▪ aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen

Tabelle 1 Vergleich der nach Art. 13 und Art. 14 DSGVO bereitzustellenden Informationen

Wenn der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten ursprünglich erhoben wurden, so stellt er der betroffenen Person auch hier nach Art. 14 Abs. 4 DSGVO vor einer Weiterverarbeitung erweiterte Informationen zur Verfügung. Art. 14 Abs. 5 DSGVO enthält Ausnahmeregelungen und bestimmt dementsprechend diejenigen Fälle, in denen Absatz 1, 2, 3 und 4 keine Anwendung finden. Weitere Ausnahmen finden sich in den §§ 29 Abs. 1 S. 1 und 33 BDSG.

5.2.2.3 Informationspflichten beim Einsatz von KI-Systemen

Die DSGVO adressiert KI-Systeme nicht direkt, aber gebietet in Art. 13 Abs. 2 Buchst. f DSGVO zusätzliche Informationen über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – „*zumindest in diesen Fällen*“ – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person bereitzustellen.

Automatisierte Entscheidungsfindung: bezeichnet die Fähigkeit eines Systems Entscheidungen durch Nutzung technologischer Mittel zu fällen, ohne eine menschliche Beteiligung.[266]

Profiling: Der Begriff des Profilings wird in Art. 4 Nr. 4 DSGVO definiert:[267]

> „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen

Die Informationspflicht scheint auch Profilingmaßnahmen zu umfassen, die eine automatisierte Entscheidung nicht ausschließlich bestimmen oder überhaupt nicht zu einer automatisierten Entscheidung führen

[266] *Artikel-29-Datenschutzgruppe*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), S. 8.
[267] Siehe ausführlich hierzu: Abschnitt 7.1.1.

sollen (bspw. Profiling zu Werbezwecken).[268] Jedenfalls gilt der Grundsatz, dass die betroffenen Personen von der Verarbeitung ihrer personenbezogenen Daten nicht überrascht werden dürfen, auch für das Profiling im Allgemeinen.[269]

Aus der Formulierung „zumindest in diesen Fällen" könnte zwar gefolgert werden, dass weitere unterhalb der Schwelle des Art. 22 DSGVO liegende automatisierte Verarbeitungen unter die Regelung fallen. Allerdings bleibt offen, nach welchen Kriterien diese zu bestimmen wären. Da es sich um eine bußgeldbewehrte Vorgabe handelt, sprechen rechtsstaatliche Gründe gegen eine Ausweitung.[270]

Aussagekräftige Informationen über die involvierte Logik: Die involvierte Logik soll den Aufbau, die Struktur und den Ablauf der Datenverarbeitung umfassen.[271] Zudem werden Methoden und Kriterien der Datenverarbeitung genannt, etwa die Funktionsweise des Algorithmus, nicht hingegen die Verarbeitungsergebnisse – diese liegen zum relevanten Zeitpunkt ohnehin noch nicht vor.[272] Als unklar wird bemängelt, ob der konkrete Algorithmus offen gelegt werden muss.[273] „Aussagekräftig" lässt sich in diesem Zusammenhang so interpretieren, dass die automatisierte Einzelentscheidung der betroffenen Person auf eine Art und Weise erläutert wird, dass diese ihre Rechte nach Art. 22 DSGVO wahrnehmen kann.[274] Notwendig ist eine dem menschlichen Verstand zugängliche Erklärungsform.[275] Insofern sollte bei Darstellung von Algorithmen, diese um erklärende Bestandteile ergänzt werden, da die betroffene Durchschnittsperson mit technischen Beschreibungen und Daten überfordert sein wird.[276] Anderer fordern auch mit Blick auf die Verständlichkeit nur das Grundprinzip (wesentliche Gründe, Informationsquellen, deren Relevanz, Gewichtung, etc.) zu erläutern – nicht hingegen die Berechnungsformel selbst oder den Algorithmus offenlegen oder aufwendig erklären zu müssen.[277] Zwar besteht ein zentrales Problem bei KI-Systemen in der *vollständigen Erklärbarkeit* einerseits im Hinblick auf darstellerische und verständnisbezogene Grenzen, andererseits aber auch durch ein gewisses Maß an Unvorhersehbarkeit bei selbstlernenden Algorithmen.[278] Hier lässt sich allerdings anführen, dass der Einsatz solcher Algorithmen ausgeschlossen sein sollte, wenn diese nicht mal im Ansatz verstanden sind, dass die begrenzten Informationspflichten der Art. 13 und 14 DSGVO erfüllt werden könnten.[279] Gleichzeitig sollte im Sinne eines „innovationsoffenen Verständnisses des Datenschutzrechts" keine prohibitiv wirkenden Maßstäbe an die aussagekräftigen Informationen angelegt werden.[280]

Tragweite und die angestrebten Auswirkungen: Der Verantwortliche sollte darüber aufklären, *worüber* aufgrund der Datenverarbeitung entschieden werden soll, skizzieren welche Entscheidungsmöglichkeiten dabei bestehen und welche Verarbeitungsergebnisse zu welcher Entscheidung führen können.[281]

---

[268] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 16; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 52; *Franck,* in: Gola DS-GVO, Art. 13 Rn. 27; a.A. *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 31 m.w.N.

[269] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 22.

[270] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (282). Es handelt sich vermutlich um ein redaktionelles Versehen bei der Übernahme von Vorschriften der Datenschutz-Richtlinie von 1995. Offene Formulierungen eröffneten den Mitgliedstaaten Umsetzungsspielräume, welche allerdings unter der DSGVO für die Informationspflichten nicht bestehen.

[271] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 16.

[272] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 54.

[273] *Franck,* in: Gola DS-GVO, Art. 13 Rn. 26. Ablehnend: *Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 31b. mit Verweis auf den Schutz von Geschäftsgeheimnissen. Gegen eine Bereitstellungspflicht der Berechnungsformel bzw. des Algorithmus: *Gausling*, DSRITB 2018, 519 (537).

[274] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 16.

[275] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (285).

[276] *Franck,* in: Gola DS-GVO, Art. 13 Rn. 26.

[277] *Gausling*, DSRITB 2018, 519 (537).

[278] *Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 31e; *Fraunhofer IAIS*, Vertrauenswürdiger Einsatz von Künstlicher Intelligenz, S. 11.

[279] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 16.

[280] *Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 31e; *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (285 f.).

[281] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 55.

Grenzen? Umstritten ist, ob der Verweis auf Geschäftsgeheimnisse die Informationspflicht begrenzen kann.[282] So wird vertreten, dass Geschäftsgeheimnisse oder das Urheberrecht an Software die Informationspflicht zwar einschränken können, sie aber nicht vollständig entfallen lassen. [283] Andere wiederum argumentieren damit, dass anders als die alte Rechtslage in den Art. 13 und 14 DSGVO keine besondere Ausnahme für Geschäftsgeheimnisse niedergelegt ist und im Rahmen der Regelungsbefugnis des Art. 23 DSGVO keine Ausnahme geschaffen wurde.[284] So bliebe nur der Verweis auf Treu und Glauben in Art. 5 Abs. 1 lit. a DSGVO in der Form, dass eine allgemeine Rechtsgüterabwägung möglich sei.[285] Da eine pauschale Bevorzugung von Unternehmensinteressen gegenüber Betroffeneninteressen sowohl der GrCh als auch der DS-GVO fremd sind, seien Geschäftsmodelle schlichtweg nicht realisierbar, die mit grundlegenden Transparenzanforderungen nicht in Einklang zu bringen sind.[286]

„Recht auf Erklärbarkeit?“ Die Gefahren automatisierter, maschineller Entscheidungen wird gerade darin gesehen, dass die Ergebnisse nicht ohne hohen technischen Aufwand erklärt und nachvollzogen werden können.[287] Eine fehlende Reflexion kann die unkritische Übernahme (auch fehlerbehafteter) Entscheidungen begünstigen – bis hin zur „Digital Unconsciousness“.[288] Ohne Rechtspflicht drohen einer transparenten und nachvollziehbaren KI zu verhallen. Ein Recht auf „*Erklärbarkeit*“ kann in diesem Sinne verstanden werden, als ein situationsangemessener „Grad, in dem ein Mensch die Ursache einer Entscheidung verstehen kann“.[289] Erklärungen könnten sich dabei – je nach technischer Machbarkeit – beziehen auf:

Inhaltliche Dimension	Zeitliche Dimension
– das gesamte Modellverhalten (global) – individuelle Einzelentscheidung (lokal)	– Vorabinformationen (ex ante) – Begründung der spezifischen Lösung (ex post)

Diskutiert wird, ob aus Art. 13 Abs. 2 Buchst. f i.V.m. Art. 22 Abs. 3 und ErwGr 71 DSGVO ein „Recht auf Erklärbarkeit“ folgt.[290] Eine Erklärbarkeit würde voraussetzen, dass der:die Verwender*in die Funktionsweise des Systems und gegebenenfalls auch die konkrete Entscheidungsfindung im Einzelfall nachvollziehen kann, obwohl die künstlichen neuronalen Netze oftmals als „Black-Box“-Systeme bezeichnet werden, da der Lösungsweg bislang nur mit hohem technischen Aufwand nachvollziehbar war.[291] Neben den nach Art. 13, 14 DSGVO bereitzustellenden Vorabinformationen besagt ErwGr. 71 S. 4 zur Auslegung der Rechte nach Art. 22 Abs. 3 DSGVO, dass zu den angemessenen Garantien die „*Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung*“ zählt. Daraus könnte das Bestehen einer einzelfallabhängigen nachträglichen und einzelfallbezogenen Erklärungspflicht hinsichtlich spezifischer Verarbeitungsvorgänge abgeleitet werden.[292] Als Gegenargumente werden einerseits die technischen Schwierigkeiten bei der Offenlegung des

[282] Befürwortend: *Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 31b m.w.N. *Gausling*, DSRITB 2018, 519 (537 f.).
[283] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 16.
[284] *Franck,* in: Gola DS-GVO, Art. 13 Rn. 28; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 54.
[285] *Franck,* in: Gola DS-GVO, Art. 13 Rn. 28.
[286] *Franck,* in: Gola DS-GVO, Art. 13 Rn. 28
[287] Vgl. *Schefzig*, DSRITB 2018, 491 (493).
[288] *Wischmeyer*, AöR 2018, 1 (21) m.w.N.
[289] *Käde/Maltzan*, CR 2020, 66 (68).
[290] *Kumkar/Roth-Isigkeit*, JZ 2020, 277; *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 31d; *Wachter u. a.*, International Data Privacy Law 2017, 76; *Casey u. a.*, Berkeley Tech. LJ 2019, 143.
[291] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (277); vgl. *Fraunhofer IAIS*, Vertrauenswürdiger Einsatz von Künstlicher Intelligenz, S. 11; *Käde/Maltzan*, CR 2020, 66 (67).
[292] *Casey u. a.*, Berkeley Tech. LJ 2019, 143 (157).

Entscheidungsweges und legitime Interessen am Schutz von Geschäftsgeheimnissen angeführt.[293] Im Hinblick auf die technische Ebene ist zu konstatieren, dass die Zielsetzung die innere Struktur für technische Laien nachvollziehbar zu machen kaum über die Offenlegung von Rohdaten und Algorithmen gelingen kann, da die Systeme als zu komplex und dynamisch gelten.[294]

Da sich keine entsprechende Erwähnung der Erklärungspflicht im Normtext selber findet und die Erwägungsgründe nur zur Auslegung der „angemessenen Maßnahmen" herangezogen werden können, gibt es derzeit keine zwingende Vorgabe für eine rechtfertigende Erläuterung der Entscheidung.[295] Insbesondere fällt ein solches Recht nicht unter die Mindestgarantien nach Art. 22 Abs. 3 DSGVO, welche bei einer ausnahmsweise zulässigen automatisierten Einzelfallentscheidung stets zu beachten sind.[296] Erforderliche „angemessene Maßnahmen" können im Einzelfall aber über die Mindestgarantien hinausgehen. Offen ist derzeit noch, für welche Fälle eine nachträgliche und einzelfallbezogene Erklärungspflicht erforderlich wäre. Zwingenden Charakter haben hingegen die Informations- und Auskunftsrechte nach Art. 13, 14 und 15 DSGVO und hier insbesondere die Mitteilung der involvierten Logik. *Wachter/Mittelstadt/Floridi* kommen daher zum Ergebnis, die DSGVO gewähre ein Recht auf Information (right to be informed) aber kein Recht auf Erklärbarkeit (right to explanation).[297] *Kumkar/Roth-Isigkeit* plädieren für die Annahme einer Pflicht zur Offenlegung von möglichen *ex-ante*-Entscheidungskriterien (Ankündigung der bevorstehenden automatisierten Entscheidung und abstrakte Erläuterung allgemeiner Funktionsweise), nicht aber *ex post* die Offenlegung des Prozesses der Entscheidungsfindung und Abwägung im Einzelfall.[298]

Insgesamt verbleiben Fragestellungen zur Erklärungstiefe. *Martini* will diese entsprechend des risikobasierten Ansatzes an das Diskriminierungsrisiko und die Persönlichkeitsgefährdung koppeln.[299] Sinn und Zweck der Regelungen ist es dagegen, die betroffenen Personen in die Lage zu versetzen, das Risiko einzuschätzen und die Geltendmachung von Rechten zu prüfen, bspw. wenn ein Entscheidungsprozess an unzulässige Kriterien anknüpft. Denn wenn die fehlende Erkennbarkeit von persönlichkeitsrechtsrelevanten Entscheidungen dazu führt, dass Rechte praktisch eingeschränkt oder Ansprüche unzureichend wahrgenommen werden, erscheint es rechtsstaatlich geboten regulierend gegen zu wirken.[300] Fundamental ist daher zunächst die Kenntnis, *dass* eine Entscheidung auf KI basiert. Des Weiteren sollten ihnen die damit verbundenen Risiken und Grenzen des Systems bewusst werden, um ihre Anfechtungsmöglichkeiten wahrnehmen zu können. Verantwortliche sollten sich dabei daran orientieren, ob die von ihnen bereitgestellten Informationen dieser Zielsetzung gerecht werden.

5.2.2.4 Formvorschriften

Nach Art. 12 Abs. 1 S. 2 DSGVO erfolgt die Übermittlung der Informationen schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Dies führt dazu, dass der Verantwortliche eine freie Wahl der Form hat, es besteht auch kein Vorrang der schriftlichen vor der elektronischen Form (technikneutral).[301] Weniger relevant

[293] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (277, 285). Die Autor*innen weisen allerdings selbst darauf hin, dass allein aus technischen Schwierigkeiten auf die Begrenzung von Rechtspflichten zu schließen zum Fehlschluss des Faktischen über das Normative führen kann.
[294] *Käde/Maltzan*, CR 2020, 66 (67).
[295] *Wachter u. a.*, International Data Privacy Law 2017, 76 (77).
[296] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (281).
[297] *Wachter u. a.*, International Data Privacy Law 2017, 76 (78).
[298] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (278).
[299] *Martini*, JZ 2017, 1017 (1020).
[300] *Wischmeyer*, AöR 2018, 1 (22).
[301] *Quaas,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 12 Rn. 27; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 12 Rn. 16; *Greve,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 12 Rn. 18.

im Rahmen der Nutzung elektronischer Kommunikationswerkzeuge ist die in Art. 12 Abs. 1 S. 3 DSGVO normierte Möglichkeit einer mündlichen Informationsbereitstellung. Grundsätzlich wird für eine gewisse Fixierung der Mitteilung plädiert.[302] Empfohlen werden zudem insbesondere bei sehr langen Datenschutzerklärungen sog. Multi-Layered Notices, also der Darstellung in mehrschichtiger Form, sodass sich betroffene Personen einen schnellen Überblick verschaffen können.[303]

Datenschutzerklärungen: Diese ist auf einer auf einer Webseite nur dann leicht zugänglich, wenn sie nicht nur auf der Startseite, sondern auf jeder Folgeseite verlinkt ist, über die personenbezogene Daten erhoben werden. [304] Handelt es sich um eine App muss die Erklärung im jeweiligen App-Sore vor Installation der App einsehbar sein. Eine Verlinkung ist dabei ausreichend. Es sollte allerdings darauf geachtet werden, dass nicht zu viele Klicks oder ein intensives Scrollen erforderlich ist, um an die Erklärung zu gelangen.[305] Des Weiteren muss die Datenschutzerklärung innerhalb der App verfügbar gehalten werden. Empfohlen wird hier, nie mehr als zwei „Klicks“ zum Abruf vorzusehen.[306]

Die Informationsbereitstellung muss präzise, verständlich und leicht zugänglich sein und dabei in einer klaren und einfachen Sprache gehalten. Optimal ist eine kurze und bündige Darstellung mit einer gut strukturierten Gliederung, um eine Informationsüberflutung zu vermeiden.[307] Hierfür sollte auch eine klare Trennung von anderen Sachverhalten (wie bspw. den Nutzungs- und Lizenzbestimmungen) gegeben sein.[308] Im Hinblick auf die Verständlichkeit und den Zuschnitt auf die Zielgruppe ist zu verlangen, dass für den deutschsprachigen Raum auch eine Datenschutzerklärung in deutscher Sprache vorgehalten wird.[309]

Bildsymbole: Einen innovativen Ansatz enthalten Art. 12 Abs. 7 und 8 DSGVO mit Regelungen zur möglichen Verwendung von standardisierten Bildsymbolen – allerdings ohne diese näher zu konkretisieren. Des Weiteren sind Regelungen zur Umsetzung durch die EU-Kommission in Form von delegierten Rechtsakten aktuell noch nicht vorhanden. Will ein Verantwortlicher Piktogramme oder andere grafische Elemente einsetzen, sind diese stets neben der textuellen Informationsbereitstellung zu sehen. Eine Pflicht zusätzlich Bildsymbole zu verwenden besteht nicht.[310]

5.2.2.5 Ausnahmen

Verfügt die betroffene Person bereits über alle relevanten Informationen, so finden die Absätze 1, 2 und 3 des Art. 13 DSGVO (bzw. 1-4 des Art. 14 DSGVO) hingegen keine Anwendung (Art. 13 Abs. 4 und Art. 14 Abs. 5 Buchs. a DSGVO). Der Verantwortliche hat zu beweisen, dass die Informationen bereits bekannt sind.[311] Gestritten wird darüber, ob Informationspflichten nur *insgesamt* oder auch *teilweise* entfallen können.[312] Im

[302] *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 12 Rn. 38; *Quaas,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 12 Rn. 27.
[303] *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 12 Rn. 39.
[304] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 19.; *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 8.
[305] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 8.
[306] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 19.
[307] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 7. Eine Datenschutzerklärung mit mehr als 50 Bildschirmseiten für einen Smart-TV ist unzumutbar: LG Frankfurt, Urteil vom 10.06.2016 – 2-3 O 364/15.
[308] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 7.
[309] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 10.
[310] *Grewe,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 12 Rn. 32 m.w.N.
[311] *Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 94.
[312] *Knyrim,* in: Ehmann/Selmayr - DSGVO Art. 13 Rn. 68; vgl. auch *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 13 Rn. 10.

Rahmen der elektronischen Kommunikation dürfte dieser Ausnahme keine besondere Bedeutung zukommen, da sich die Informationstexte leicht verlinken lassen.[313]

In Art. 14 Abs. 5 DSGVO sind weitere Ausnahmen geregelt, wie die Unmöglichkeit, ein unverhältnismäßig hoher Aufwand, die ausdrückliche Regelung durch Rechtsvorschriften sowie berufliche Geheimhaltungspflichten. Unverhältnismäßigkeit kann angenommen werden, wenn die Informationspflicht die Verwirklichung der Verarbeitungsziele voraussichtlich unmöglich macht oder ernsthaft beeinträchtigt.[314] Anhaltspunkte zur Bestimmung liefert ErwGr. 62 S. 3 DSGVO: die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien. Bezüglich dieser Ausnahmen von der Informationspflicht ist umstritten, ob diese analog auch für Art. 13 DSGVO herangezogen werden könnten. [315] Mit Verweis auf ErwGr. 62, welcher nicht nach Erhebung bei der betroffenen Person oder bei Dritten differenziert, wird es zumindest als diskutabel aufgeworfen, ob eine Analogie möglich wäre.[316] Dagegen wird eingewandt, dass es bereits an einer planwidrigen Regelungslücke fehle und die Interessenlagen andere seien. [317] Bei einer Erhebung bei der betroffenen Person sind kaum Fälle denkbar, in welchen Unmöglichkeit anzunehmen wäre.[318]

5.2.3 Auskunftsrechte

Das Auskunftsrecht des Art. 15 DSGVO steht den betroffenen Personen zu und umfasst zum einen das Recht eine Bestätigung zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden, und sofern dies der Fall ist, das Recht auf Auskunft über diese personenbezogenen Daten sowie die Mitteilung der:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden,
- Empfänger(-Kategorien), denen Daten offengelegt werden/wurden,
- Speicherdauer oder Kriterien für deren Festlegung,
- Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie Widerspruchsrecht,
- Beschwerderechte bei Aufsichtsbehörde,
- Herkunft der Daten, sofern nicht bei der betroffenen Person selbst erhoben, und
- bei Bestehen einer automatisierten Entscheidungsfindung gemäß Art. 22 DSGVO: aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Der Auskunftsanspruch besteht auch für die Verarbeitung personenbezogener Daten im Arbeitsverhältnis.[319] Die Reichweite über welche Daten Auskunft zu erteilen ist, hängt auch von der Bestimmung des Personenbe-

[313] Siehe kritisch für den Offline-Bereich: *Knyrim,* in: Ehmann/Selmayr - DSGVO Art. 13 Rn. 68.
[314] *Niemann/Kevekordes*, CR 2020, 179 (181).
[315] *Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 95.
[316] *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 35.
[317] *Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 95; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 13 Rn. 11; *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 22.
[318] Franck beschreibt hingegen die Fallkonstellation einer unaufgeforderten Kontaktaufnahme durch die betroffene Person mit Unmöglichkeit einer Rückantwort aufgrund von Zugangshindernissen bei der betroffenen Person: *Franck,* in: Gola DS-GVO, Art. 13 Rn. 45. In solchen Ausnahmefällen dürfe es nicht dem Verantwortlichen Nachteile bereiten.
[319] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 172; *Düwell/Brink*, NZA 2016, 665 (667).

zugs ab, denn nur über die konkret verarbeiteten personenbezogenen Daten ist Auskunft zu erteilen (vgl. Abschnitt 2.2.1 zum Personenbezug und Abschnitt 4.1.1.1 zum Begriff der Verarbeitung).[320] Der BGH positionierte sich jüngst gegen eine teleologische Reduktion, welche die erfassten Informationen nach Signifikanz einschränken würde.[321] Auch ist es unerheblich, ob die Information dem Auskunftsersuchenden bereits bekannt ist.[322]

Auskunftsberechtigte sind nach ErwGr. 63 S. 7 DSGVO berechtigt, ihr Auskunftsersuchen auf bestimmte Informationen oder Verarbeitungsvorgänge zu beziehen.[323] Eine Beschäftigte kann bspw. ihren zunächst umfassend bestehenden Auskunftsanspruch auf personenbezogene Leistungs- und Verhaltensdaten einschränken. Ferner sollen Betroffene ihr Recht „problemlos“ und in „angemessenen“ Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (ErwGr. 63 S. 1 DSGVO). Art. 12 und 15 DSGVO regeln zudem das Verfahren, wie und von wem ein Auskunftsersuchen zu stellen ist und wie und in welcher Form der Verantwortliche hiermit umzugehen hat. Das Auskunftsrecht steht der betroffenen Person zu und kann durch einen Antrag an den Verantwortlichen wahrgenommen werden, d.h. die betroffene Person muss ihr Recht aktiv wahrnehmen.[324]

Die DSGVO schreibt für das Auskunftsrecht – abgesehen von der Frage der Antwort auf elektronische Auskunftsersuchen – keine spezifische Umsetzung vor, was dem Grundsatz der Technikneutralität der DSGVO entspricht.[325] Nichtsdestotrotz bietet ErwGr. 63 S. 4 DSGVO einen Impuls, wie Verantwortliche das Recht auf Auskunft umsetzen könnten:

> **ErwGr. 63 S. 4 DSGVO** Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.

5.2.3.1 Recht auf Kopie der verarbeiteten personenbezogenen Daten

Art. 15 Abs. 3 DSGVO schreibt ferner vor, dass und in welcher Form eine Kopie über die Daten der betroffenen Person zur Verfügung zu stellen sind. Dieses Recht auf Kopie kann als ein mit der Geltung der DSGVO neu eingeführtes Recht bezeichnet werden.[326] Wurde der Antrag elektronisch gestellt wird, sind die Informationen on einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sich nichts anderes ergibt. Erst für „weitere Kopien“, welche die betroffene Person beantragt, darf ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangt werden. Um eine exzessive Nutzung dieses Rechts zu verhindern sind die Kosten für weitere Kopien von der betroffenen Person zu tragen. Der Unterschied zwischen Auskunft nach Art. 15 Abs. 1 DSGVO und dem Recht eine Kopie zu erhalten liegt in der Art der Darstellung der bereitzustellenden Informationen, denn ersteres enthält zunächst keine Vorgaben hinsichtlich der Präsentation der Daten.[327] Letztere kommt einer wahrheitsgetreuen Abbildung der tatsächlichen Verarbeitungsprozesse nahe.[328]

---

[320] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 22; *Engeler/Quiel*, NJW 2019, 2201 (2202). Zur Abgrenzung vgl. auch LG Köln, Teilurteil vom 18.03.2019 - 26 O 25/18, Rn. 15; KG, Beschluss vom 23.10.2018 – 6 U 45/1.
[321] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 22.
[322] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 25.
[323] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 176.
[324] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 1; ausführlich zum Auskunftsrecht: *Engeler/Quiel*, NJW 2019, 2201.
[325] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 44a.
[326] *Engeler/Quiel*, NJW 2019, 2201 (2201).
[327] *Engeler/Quiel*, NJW 2019, 2201 (2202).
[328] Beispiele bei: *Engeler/Quiel*, NJW 2019, 2201 (2203). Eine Aufbereitung oder Modifikation der personenbezogenen Daten kann nicht verlangt werden: *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 40.

5.2.3.2 Auskunftsrechte beim Einsatz von KI-Systemen

Gemäß Art. 15 Abs. 1 Buchst. h DSGVO hat die betroffene Person ein Recht auf Auskunft über folgende Informationen:

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

Auch insofern hat der Verantwortliche Transparenz über von Art. 22 DSGVO erfasste Tatbestände herzustellen. Während die Informationspflicht sich auf eine geplante automatisierte Entscheidungsfindung bezieht, ist hier über automatisierte Entscheidungen zu beauskunften, die bereits stattgefunden haben.[329] Umstritten ist, ob damit über die Informationspflichten der Art. 13, 14 DSGVO hinausgehend mehr Informationen über die spezifischen Umstände der Einzelfallentscheidung bereitgestellt werden müssen. Der deckungsgleiche Wortlaut sowie die gewählte Formulierung der „angestrebten" Auswirkungen werden gegen eine solche Interpretation ins Feld geführt.[330]

5.2.3.3 Ausnahmen

Es bestehen unterschiedlichste Szenarien, in denen eine Auskunft nicht erteilt werden kann:

Mangelnde Identifizierbarkeit: In Art. 11 DSGVO wird der Sonderfall geregelt, dass der Verantwortliche die betreffende Person nicht (mehr) identifizieren kann. Der Verantwortliche soll nicht verpflichtet werden, mehr Daten als unbedingt erforderlich zu erheben und/oder zu speichern, um die Betroffenenrechte umzusetzen. Dies entspricht den Grundsätzen der Datenminimierung und Speicherbegrenzung.[331] Macht die betroffene Person ihr Auskunftsrecht geltend, ist sie hierüber zu informieren, da die weiteren Betroffenenrechte in Art. 15 bis 20 DSGVO keine Anwendung mehr finden und nicht mehr wahrgenommen werden können, sofern eine Zuordnung beispielsweise eines Auskunftsersuchens zu den vorhandenen Daten aufgrund der fehlenden Zuordenbarkeit nicht mehr möglich ist. Gemäß Art. 12 Abs. 2 S. 2 DSGVO darf sich in diesen Fällen des Art. 11 Abs. 2 DSGVO der Verantwortliche allerdings nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte nach den Art. 15 bis 22 DSGVO tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren. Die betroffene Person kann allerdings zusätzliche Informationen bereitstellen, die ihre Identifizierung ermöglichen.[332]

Diese Ausnahme entfaltet besonders bei der Möglichkeit „anonymer" oder pseudonymer Nutzung von Kommunikationswerkzeugen praktische Bedeutung und ist der weiten Definition personenbezogener Daten geschuldet. Hier können rechtlich gesehen grundsätzlich Identifizierungsmöglichkeiten anzunehmen sein, sodass es sich um personenbezogene Daten handelt, der Verantwortliche diese Mittel zur Identifizierung aber nicht nutzt.[333] Die Befreiung von den Pflichten der Art. 15 ff. DSGVO greift allerdings nur, wenn es dem Verant-

[329] *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 16.
[330] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (283).
[331] *Wolff,* in: BeckOK DatenschutzR Art. 11 Rn. 4, 8; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 11 Rn. 1.
[332] In diesem Fall leben die Pflichten der Art. 15 ff. DSGVO wieder auf: *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 11 Rn. 10.
[333] *Wolff,* in: BeckOK DatenschutzR Art. 11 Rn. 12.

wortlichen nicht mit eigenen, intern verfügbaren Mitteln gelingt, eine Zuordnung des Antragstellenden vorzunehmen.[334] Zudem gilt natürlich zu bedenken, dass eine eindeutige Identifizierung nicht Klarnamen, Adresse, Geburtsdatum etc. bedeutet, sondern auf verschiedenen Wegen der Authentisierung sichergestellt werden kann, dass keine Auskunftsdaten an nicht berechtigte Personen herausgegeben werden (bspw. Missbrauch eines Pseudonyms nach Identitätsdiebstahl).[335]

Rechte und Freiheiten anderer Personen: Das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DSGVO darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen (Art. 15 Abs. 4 DSGVO). Hierzu werden auch die Rechte juristischer Personen gezählt.[336] Zu den „anderen Personen" zählt auch der Verantwortliche selbst.[337] Anders als der Auskunftsanspruch, steht das Recht auf Kopie unter einem Abwägungsvorbehalt. [338] Es wird zwar vertreten, dass sich diese Einschränkung auch auf den Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO beziehe.[339] Dies entspricht allerdings nicht dem Wortlaut.[340] Unklar ist, ob es sich bloß um ein Redaktionsversehen handelt. [341]

Das Recht auf Kopie kann folglich ausgeschlossen oder eingeschränkt sein,

- wenn in der Kopie personenbezogene Daten enthalten sind, die sich auf Dritte beziehen, sodass in einer Weitergabe eine Verletzung ihrer Datenschutz- und Persönlichkeitsrechte läge,
- wenn die Herausgabe Urheberrechte oder Geschäftsgeheimnisse berührt, wenn deren Schutz die Rechte der auskunftsstellenden betroffenen Person überwiegen (vgl. ErwGr. 63 S. 5 DSGVO),
- bei unverhältnismäßigem Aufwand sollte der Verantwortliche verlangen können, dass die betroffene Person ihr Auskunftsersuchen präzisiert (vgl. ErwGr. 63 S. 7 DSGVO), offensichtlich unbegründete oder exzessive Anfragen können abgelehnt werden (vgl. Art. 12 Abs. 5 S. 2 DSGVO).[342]

Den Verantwortlichen trifft insoweit die Beweislast einer konkreten Kollisionslage (die bloße Besorgnis der Gefährdung dieser Rechte reicht nicht) und darf nach herrschender Meinung nicht jegliche Auskunft verweigern, sondern die Mitteilung entsprechend kürzen (z.B. Teilkopie, Schwärzungen, etc.).[343] Auch dieser Ausschluss dürfte für elektronische Kommunikationsdienste von erheblicher Bedeutung sein, da zumeist die Kommunikationspartner natürliche Personen sind und damit Datenschutzrechte geltend machen können. Ein weiteres Beispiel könnten übermittelte Medien sein. Hier könnten die Urheberrechte anderer Personen betroffen sein.

Entgegenstehende Interessen (BDSG): Beschränkungen des Auskunftsrechts durch mitgliedstaatliches Recht sind nach der Maßgabe des Art. 23 DSGVO möglich.[344] Bestimmte Beschränkungen können durchaus zur Umsetzung eines grundrechtlichen Schutzauftrags geboten sein, wie bspw. die Erfüllung der Pflichten von Berufsgeheimnisträgern, oder zum Schutz behördlicher Informanten.[345] Nach § 34 Abs. 1 i.V.m. § 29 Abs.

[334] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 11 Rn. 13 ff. *Wolff,* in: BeckOK DatenschutzR Art. 11 Rn. 15 ff.
[335] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 11 Rn. 15 f.
[336] *Engeler/Quiel*, NJW 2019, 2201 (2203).
[337] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 42.
[338] *Engeler/Quiel*, NJW 2019, 2201 (2203).
[339] So *Paal* in: Paal/Pauly - DS-GVO BDSG Art. 15 Rn. 41; *Specht,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 15 Rn. 22.
[340] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 33.
[341] So *Specht,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 15 Rn. 22.
[342] *Engeler/Quiel*, NJW 2019, 2201 (2203); *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 42b.
[343] *Specht,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 15 Rn. 24; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 42a.
[344] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 33.
[345] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 33; vgl. *Franck,* in: Gola DS-GVO, Art. 15 Rn. 36.

1 S. 2 BDSG besteht das Recht auf Auskunft nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.[346] Diese Regelungen in § 34 Abs. 1 i.V.m. § 29 Abs. 1 und 2 BDSG beruhen nach Einschätzung des LAG Baden-Württemberg auf der Öffnungsklausel des Art. 23 Abs. 1 Buchst. i DSGVO, wonach zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen Informations- und Benachrichtigungspflichten des Verantwortlichen bzw. das Auskunftsrecht betroffener Personen beschränkt werden können.[347]

5.2.4 Zwischenergebnis zu Informationspflichten und Auskunftsrechten

Für die Verwendung von KI-Systemen im Unternehmenskontext ist zunächst relevant, wer Adressat der jeweiligen Informationspflichten und wem gegenüber zu informieren ist, also wer zu den betroffenen Personen zählt. Informationspflichten werden in der Praxis häufig über die Datenschutzerklärungen erfüllt. Hier zeigt sich jedoch, dass je ausführlicher der für die Verarbeitung Verantwortliche über die Datenverarbeitungsvorgänge, deren Zwecke, die Betroffenenrechte usw. informiert, desto unübersichtlicher kann die Informationsvermittlung für die betroffene Person werden. Zumeist besteht die Schwierigkeit die Balance zwischen der Verständlichkeit und der Nachvollziehbarkeit auf der einen Seite und der Informationsüberflutung auf der anderen Seite zu halten. Insbesondere bei der Verwendung von KI-Systemen auf dem Smartphone kann dies aufgrund der geringeren Bildschirmgröße eine Herausforderung darstellen.

Bezüglich der Frage der Erklärbarkeit von KI ist noch umstritten, wieweit die Informations- und Auskunftsrechte über die involvierte Logik bei automatisierten Einzelfallentscheidungen und Profiling zu unterrichten auch ein Recht auf Detailerklärungen beinhalten. Sofern KI-Systeme nicht in den Anwendungsbereich des Art. 22 Abs. 1 DSGVO zur automatisierten Einzelfallentscheidung oder unter Profiling i.S.d. Art. 4 Nr. 4 DSGVO fallen, folgen aus der DSGVO keine gesteigerten Transparenzpflichten. Solche könnten in Zukunft aber mit einer KI-Regulierung etabliert werden (siehe Abschnitt 7).

Auskunftsersuchen können betroffene Personen an den Verantwortlichen stellen – dies könnten bei Einsatz von KI im Beschäftigungsverhältnis die Arbeitgeber*innen und/oder KI-Systemanbieter*innen sein, je nachdem wie die Verantwortlichkeit gelagert ist (vgl. Abschnitt 2.1.2). Der Verantwortliche kann zur Erfüllung seiner korrespondierenden Auskunftspflichten einen Auftragsverarbeiter, der in die Verarbeitung involviert ist, einbeziehen. Bei einer gemeinsamen Verantwortlichkeit müssen die jeweiligen Verantwortlichen Stellen dafür Sorge tragen, dass die notwendigen Informationen an die betroffene Person übermittelt werden. In Kommunikationskontexten ist im Hinblick auf den Schutz der Rechte Dritter zu beachten, dass Inhalte, die weitere Personen betreffen, von der Bereitstellung einer Kopie ggf. ausgenommen werden müssen. Festzuhalten bleiben als wesentliche Parameter zur Möglichkeit eines Auskunftsersuchens:

- **Antrag:** keine Formerfordernisse oder Begründung erforderlich
- **Frist:** Beantwortung eines Auskunftsersuchens innerhalb eines Monats
- **Kosten:** Auskunftserteilung unentgeltlich (Ausnahme Missbrauchsfälle)
- **Form:** grundsätzlich formfrei; in elektronischer Form, sofern Antrag elektronisch erfolgte (und kein anderes Format gewünscht)

[346] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 179.
[347] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 179.

5.3 Zweckbindung

Bereits in Art. 8 Abs. 2 EU-GrCh („festgelegte Zwecke“) findet sich der Grundsatz der Zweckbindung.[348] Aufgrund der unmittelbaren Wechselwirkung zu den weiteren Datenschutzgrundsätzen, ist der Grundsatz der Zweckbindung eines der zentralen Prinzipien des europäischen und deutschen Datenschutzrechts und ist zudem unmittelbarer Ausfluss des grundrechtlich geschützten Rechts auf informationelle Selbstbestimmung.[349] Er wird als Ausdruck des Grundsatzes der Verhältnismäßigkeit verstanden.[350]

> **Art. 5 Abs. 1 Buchst. b DSGVO** Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Dem Grundsatz der Zweckbindung folgend sind Zwecke im Vorfeld der Verarbeitung so zu formulieren, dass sie eindeutig sind. Hiermit soll sichergestellt werden, dass sich Verantwortliche *vor* der Verarbeitung bewusstwerden, welches Ziel mit der Verarbeitung verfolgt wird und dies den betroffenen Personen im Rahmen der Informationspflichten kommunizieren können. Des Weiteren dürfen personenbezogene Daten nicht auf eine Art und Weise weiterverarbeitet werden, die mit dem ursprünglich festgelegten Zweck nicht vereinbar ist.[351] Eine Datensammlung „auf Vorrat“ für spätere KI-Trainings zu noch unbekannten Zwecken widerspricht eindeutig dem Grundsatz der Zweckbindung.[352]

5.3.1 Zweckfestlegung

Um prüfen zu können, ob sich eine Datenverarbeitung (noch) im festgelegten Zweck bewegt, oder bereits eine Zweckänderung vorliegt, ist es entscheidend, wie konkret Verarbeitungszwecke festgelegt werden müssen. Entsprechend des risikobasierten Ansatzes[353] der DSGVO wird vertreten, dass sich auch der Konkretisierungsgrad der Zweckfestlegung am Risiko orientieren sollte, d.h. bei geringen Risiken könnten Zwecke weiter gefasst werden als bei risikobehafteten Verarbeitungsarten oder -kontexten.[354] Es ist durchaus möglich, mehrere Zwecke zu benennen, zu pauschal gehaltene Zweckangaben sollen hingegen nicht genügen.[355]
Art. 5 Abs. 1 Buchst. b DSGVO benennt die folgenden Kriterien für die Zweckfestlegung:

- **Festgelegt:** beschreibt die Erforderlichkeit einer hinreichenden Konkretisierung der verfolgten Zwecke. Diese ist relevant, um Ziel und Umfang einer Datenverarbeitung klar und präzise genug einzugrenzen, dass bspw. im Rahmen der Informationspflichten ausreichend Transparenz erreicht wird, die Erforderlichkeit einer Datenverarbeitung zur Zielerreichung prüfbar ist, im Rahmen der Einwilligung die Tragweite der Einwilligungserklärung durch die betroffene Person abgeschätzt werden kann oder im

[348] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 57.
[349] *Culik/Döpke*, ZD 2017, 226 (227); *Gausling*, DSRITB 2018, 519 (532). Vgl. zur Bedeutung des Verarbeitungszwecks: *Raabe/Wagner*, Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data, S. 16 f.; BVerfGE 65, 1 – Volkszählungsurteil.
[350] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 57 ff.
[351] Siehe hierzu: *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203.
[352] *Niemann/Kevekordes*, CR 2020, 17 (20).
[353] Zum risikobasierten Ansatz: *Bieker u. a.*, DuD 2018, 492 (492 f.); *Veil*, ZD 2015, 347 (347 ff.); *Schröder*, ZD 2019, 503; *Voigt,* in: Konzerndatenschutz Teil 3, Kapitel 2 Grundsätze der Verarbeitung nach der DSGVO, Rn. 14; *Martin u. a.*, DuD 2020, 149 (150 f.).
[354] *Grafenstein, von*, DuD 2015, 789; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 5 Rn. 14. Vgl. auch ableitend aus einer Verhältnismäßigkeitsprüfung: *Niemann/Kevekordes*, CR 2020, 17 (21).
[355] *Culik/Döpke*, ZD 2017, 226 (227).

Rahmen der Interessenabwägung die in Verhältnis zu setzenden Interessenlagen hinreichend klar definiert sind.[356]

- **Eindeutig:** steht auch für das „Merkmal des Erklärens“ (dies wird mit dem englischen Begriff des „explicit“ deutlicher).[357] Die Angabe eines Zwecks soll unmissverständlich und unzweideutig zum Ausdruck kommen.[358]
- **Legitim:** der gewählte Zweck darf nicht im Konflikt mit der Rechtsordnung stehen.[359]

Die Angabe eines Zwecks hat folglich weitreichende Folgen, da die Zielsetzung entscheidenden Einfluss auf die Art und Dauer der Verarbeitung personenbezogener Daten hat.[360] Die Verarbeitung personenbezogener Daten ist grundsätzlich nur insoweit zulässig, wie sie vom gewählten Zweck getragen wird.

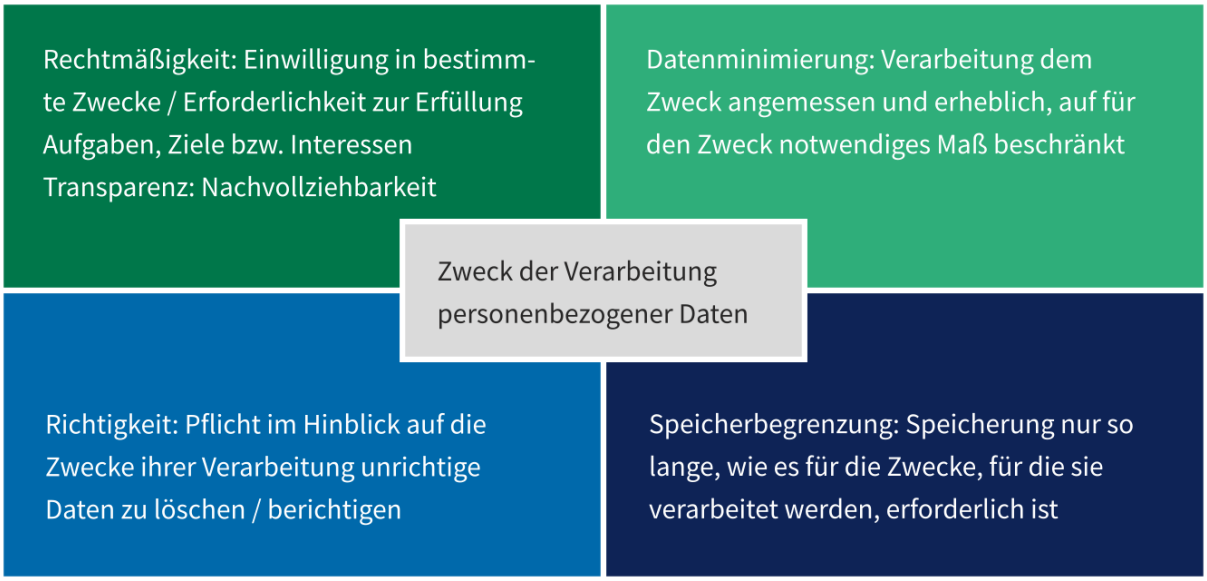


Abbildung 9 Wechselbeziehung des Zweckbindungsgrundsatzes zu anderen Datenschutzgrundprinzipien

Die betroffene Person muss anhand der Zweckangabe wissen können, wofür ihre personenbezogenen Daten verwendet werden sollen. Nicht ausreichend sind Angaben wie beispielsweise „für Marketingzwecke“, da die betroffene Person sich hierbei kein Bild davon machen kann, welche Verarbeitungen hier stattfinden können.[361] Verantwortliche sollten davon ausgehen, dass zu unklar formulierte Zwecke, die für die betroffene Person nicht nachvollziehbar sind, im Zweifelsfall zu ihren Lasten gehen und zu einer unzulässigen Verarbeitung führen könnten.[362]

5.3.2 Vereinbarkeit der Zwecke / Kompatibilitätstest

Die „Zweckbindung“ gilt nicht umfassend. Gleichwohl ist auch eine Zweckänderung grundsätzlich möglich, sofern eine Vereinbarkeit der Zwecke vorliegt. Art. 6 Abs. 4 DSGVO regelt die Möglichkeiten, Grenzen und

[356] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 12 ff.
[357] *Monreal*, ZD 2016, 507 (509).
[358] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 17.
[359] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 19 f.; *Monreal*, ZD 2016, 507 (509).
[360] Vgl. *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 5 Rn. 34.
[361] *Wolff,* in: BeckOK DatenschutzR, Kap. Syst. A. Prinzipien, Rn. 19.
[362] Vgl. *Helfrich* in: Handbuch Multimedia-Recht, Teil 16.1 Rn. 92; *Simitis,* in: Simitis, BDSG, § 28 Rn. 42.

Rahmenbedingungen einer Verarbeitung personenbezogener Daten zu Zwecken, die von denjenigen abweichen, zu denen die Daten ursprünglich erhoben wurden.

- Die betroffene Person hat in die Zweckänderung eingewilligt.[363]
- Eine Rechtsvorschrift der Union oder der Mitgliedstaaten erlaubt die Zweckänderung, wobei diese Vorschrift eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter Ziele darstellen muss (vgl. Art. 23 Abs. 1 DSGVO).[364]
- Es liegt eine Vereinbarkeit der Zwecke vor. Eine solche wird bspw. im Rahmen der Forschung angenommen, wobei die Reichweite dieser Forschungsprivilegierung durchaus umstritten ist.[365]
- Die Vereinbarkeit der Zwecke wird durch den sog. Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO nachgewiesen.[366]

Ergeben sich nach Erfüllung der ursprünglichen Zwecke der Verarbeitung berechtigte Interessen zur weiteren Verarbeitung, so ist zu prüfen, ob ein Fall einer zulässigen Zweckänderung nach Art. 6 Abs. 4 DSGVO vorliegt. Umstritten ist bei einer Zweckänderung auf Basis des Kompatibilitätstests, ob nur dieser durchzuführen ist, oder zusätzlich auch eine neue Rechtsgrundlage gegeben sein muss.[367] So lautet ErwGr. 50 S. 2 DSGVO „*In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten*." Hierbei soll es sich allerdings um ein redaktionelles Versehen handeln.[368] Mit Verweis auf die Entstehungsgeschichte der DSGVO und die grundrechtliche Verbürgung des Zweckbindungsprinzips wird von einigen Stimmen der Literatur trotz des Erwägungsgrundes gefordert, dass eine Weiterverarbeitung zu neuen Zwecken wie nach der bisherigen Rechtslage nur nach einer Zwei-Stufen-Prüfung aus Kompatibilitätstest und zusätzlicher Rechtsgrundlage zulässig sein soll.[369] Andere Autoren fordern hingegen kompensatorisch gesteigerte Anforderungen an Transparenz und Datenrichtigkeit.[370]

Vielfach dürfte der Streit in der Praxis dahinstehen.[371] Denn neben der Möglichkeit der Einwilligung dürften die neuen Zwecke zumeist auf der Wahrnehmung berechtigter Interessen beruhen. Die Anforderungen des Kompatibilitätstests zwischen (altem) Primär- und (neuem) Sekundärzweck überschneiden sich in einigen wesentlichen Punkten mit den Anforderungen an die Interessenabwägung.[372] Gemäß Art. 6 Abs. 4 DSGVO müssen bei einer Zweckänderung, die nicht durch Einwilligung oder eine Rechtsvorschrift bereits legitimiert ist, mindestens folgende Kriterien „berücksichtigt", d.h. geprüft werden:

- jede Verbindung zwischen den Erhebungs- und Weiterverarbeitungszwecken,
- Zusammenhang und Kontext der Erhebung, insbesondere Beziehung zwischen Verantwortlichem und betroffener Person,

[363] Kritisch im Kontext umfangreicher Datenverarbeitung: *Culik/Döpke*, ZD 2017, 226 (228).
[364] Für eine restriktive Auslegung: *Culik/Döpke*, ZD 2017, 226 (229).
[365] *Weichert*, ZD 2020, 18 (21); *Johannes/Richter*, DuD 2017, 300 (301).; für eine einschränkende Auslegung: *Roßnagel*, ZD 2019, 157 (162); *Roßnagel,* in: NK-DatenschutzR NK Datenschutzrecht Art. 5 Rn. 103 ff.
[366] Zur Entstehungsgeschichte: *Albrecht*, CR 2016, 88 (92).
[367] Zum Streit: *Schantz*, NJW 2016, 1841 (1844); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76; *Piltz*, K&R 2016, 557 (566); *Culik/Döpke*, ZD 2017, 226 (230); *Richter*, DuD 2016, 581 (584); *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3746); *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 31; *Niemann/Kevekordes*, CR 2020, 17 (24).
[368] *Richter*, DuD 2016, 581 (584); a.A. *Niemann/Kevekordes*, CR 2020, 17 (24).
[369] *Schantz*, NJW 2016, 1841 (1844); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76; a.A. *Piltz*, K&R 2016, 557 (566).
[370] *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 31.
[371] a.A. *Niemann/Kevekordes*, CR 2020, 17 (24). Sehen den Kompatibilitätstest als wesentlich flexibler als die Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO.
[372] Vgl. auch *Culik/Döpke*, ZD 2017, 226 (229).

- Art und Sensibilität der personenbezogenen Daten, insbesondere ob es sich um besondere Kategorien personenbezogener Daten oder strafrechtlich relevante Daten handelt,
- Mögliche Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person
- Einsatz geeigneter Schutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung.

Die genannten Kriterien sind nicht abschließend und nicht obligatorisch, da es sich nur um eine Pflicht zur „Berücksichtigung" handelt.[373]

Eine Verbindung zwischen ursprünglichem und neuem Zweck kann angenommen werden, wenn die Weiterverarbeitung „der nächste logische Schritt" ist.[374] Nach der Terminierung eines Vertrages wertet es der EDSA dagegen als grundsätzlich entgegen der Erwartungen der betroffenen Personen und der Grundsätze der Fairness und Zweckbindung, wenn Daten mittels eines Auswechselns der Rechtsgrundlage einfach weiterverarbeitet werden.[375] Es bestehen allerdings auch Möglichkeiten, die eine Weiterverarbeitung legitimieren. Die Löschpflichten gelten nicht, wenn die Verarbeitung für bestimmte Zwecke weiterhin erforderlich ist, einschließlich der Erfüllung einer Rechtspflicht nach Art. 17 Abs. 3 Buchst. b DSGVO oder der Begründung, Ausübung oder Abwehr von Rechtsansprüchen nach Art. 17 Abs. 3 Buchst. e DSGVO. Rechtliche Aufbewahrungsfristen sollten allerdings von Beginn an kommuniziert werden, sodass kein Fall der Zweckänderung vorliegt.

5.3.3 Zweckbindung und Data Mining im Kontext von KI-Anwendungen

Gerade für das Training künstlicher Neuronaler Netze kommt es darauf an, eine möglichst breite Datenbasis zu haben.[376] Diese zu Generieren ist oftmals kostenaufwändig, sodass sich das Thema der Weiternutzung bereits vorhandener Datenbestände in diesem Kontext geradezu aufdrängt. Zudem werden KI-Systeme oftmals gerade dafür eingesetzt, neue Strukturen und Muster in Datenbeständen zu erkennen, die zuvor unbekannt waren, wofür Daten aus unterschiedlichsten Kontexten zusammengeführt werden.[377] Da die Analyse zuvor getrennter Datensätze dazu geeignet ist, tiefere Einblicke zu gewinnen, als dies mit den Originaldatensätzen der Fall gewesen wäre, steigt die Eingriffsintensität und damit das Risiko für die Rechte und Freiheiten von der Datenverarbeitung betroffener Personen. Diesen Risiken soll der Zweckbindungsrundsatz entgegenwirken.[378] Die Weiternutzung muss sich am Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO messen.

Vorhersagemodelle und Profiling Vielfach werden KI-Systeme eingesetzt, um Prognosen und Vorhersagen über zukünftige Ereignisse zu generieren. Handelt es sich um menschliches Verhalten, könnte es sich hierbei um Profiling i.S.d. Art. 4 Nr. 4 DSGVO handeln.[379]

> „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten,

[373] *Culik/Döpke*, ZD 2017, 226 (229); *Niemann/Kevekordes*, CR 2020, 17 (24).
[374] *Gausling*, DSRITB 2018, 519 (532).
[375] *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, S. 12.
[376] *Niemann/Kevekordes*, CR 2020, 17 (18) m.w.N.
[377] *Raji*, DSB 2022, 193 (193); *Niemann/Kevekordes*, CR 2020, 17 (20).
[378] *Schefzig*, DSRITB 2018, 491 (498).
[379] *Raji*, DSB 2022, 193 (194).

> insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

Privilegierungen[380] *Raji* diskutiert, ob das KI-Training unter die Privilegierung für statistische Zwecke[381] subsumiert werden könnte: dann müsste die Phase der Erstellung eines stochastischen Modells losgelöst von späterer Implementierung und Einsatz betrachtet werden, um den Zweck auf die Erstellung statistischer Analysezwecke zu begrenzen.[382] Allerdings hob bereits 2013 die Art-29-Datenschutzgruppe hervor, dass die Anwendung des Modells auf einzelne Personen mitberücksichtigt werden muss.[383] Insofern ist der eigentliche Zweck in der Regel nicht bloß die statistische Untersuchung oder Erstellung statistischer Ergebnisse. ErwGr. 162 stellt zudem klar, dass die Privilegierung auf dem Gedanken beruht, dass das Ergebnis der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind, welchen nicht für Maßnahmen und Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.

Reallaborkonzept des KI-Verordnungsentwurfs: Im Vorschlag der EU-Kommission für eine KI-Verordnung („AI Act")[384] findet sich auch das Konzept „regulatorischer Sandkästen". Diese Reallabore sollen ein kontrolliertes Experimentierumfeld in der Entwicklungs- und Vorvermarktungsphase neuer KI-Systeme schaffen.[385] Um rechtliche Hindernisse insbesondere für KMUs und Start-ups zu beseitigen, soll eine spezifische Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten zur Entwicklung von KI-Systemen *in erheblichen öffentlichen Interesse* geschaffen werden (Art. 54 KI-VOE). Der Ansatz umfasst:

- **Eingeschränkter Geltungsbereich:** nur in bestimmten Bereichen: Strafverfolgung, öffentliche Sicherheit, Gesundheit, Umweltschutz
- **Subsidiarität:** die Ziele sind mit anonymisierten, synthetischen, nicht-personenbezogenen Daten nicht erreichbar
- **Sicherheitsvorkehrungen:** u.a. funktional getrennte, isolierte und geschützte Datenverarbeitungsumgebung; Zugriff nur für Befugte, keine Datenübermittlung an / kein Zugriff für Dritte
- **Schutz potentiell Betroffener:** Systeme dürfen keine Maßnahmen oder Entscheidungen mit Auswirkungen auf die betroffenen Personen vorsehen
- **Aufsicht:** nationale Datenschutzbehörden sollen in den Betrieb des KI-Reallabors einbezogen werden (Art. 53 Abs. 2 KI-VOE)

Die Regelung soll im Einklang mit den datenschutzrechtlichen Vorgaben zur Zweckänderung, wie Art. 6 Abs. 4 DSGVO, Art. 6 VO (EU) 2018/1725 und Art. 4 Abs. 2 JI-RL stehen. Sie würde insofern eine Rechtsvorschrift der Union bilden, welche eine Weiterverarbeitung erlaubt, sodass kein Kompatibilitätstest erforderlich ist. Das Verhältnis zu den privilegierten Verarbeitungskontexten nach Art. 5 Abs. 1 Buchst. b DSGVO wäre hingegen noch zu klären.

---

[380] Privilegierungen zu Forschungszwecken siehe: Abschnitt 9.

[381] Nach ErwGr. 162 ist unter dem Begriff „statistische Zwecke" jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten zu verstehen. Statistik ist der methodische Umgang mit empirischen Daten, vgl. *Niemann/Kevekordes*, CR 2020, 179 (180).

[382] *Raji*, DSB 2022, 193 (194).

[383] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 28 f.

[384] *EU-Kommission,* 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 21.4.2021 – COM(2021) 206 final.

[385] Vgl. ErwGr. 72 KI-VOE; *Orssich*, EuZW 2022, 254 (260).

5.3.4 Zwischenergebnis zur Zweckbindung

Das Prinzip der Zweckbindung bedeutet für die für die Verarbeitung Verantwortlichen, dass sie sich vorab vor einer Datenverarbeitung Gedanken über den Zweck der Verarbeitung der personenbezogenen Daten machen müssen. Diese Zwecke sind der betroffenen Person in einer Art und Weise zu nennen, die für diese nachvollziehbar bzw. verständlich ist.

Mit der Verfolgung eigener oder fremder Zwecke, entscheidet sich zudem die Frage nach der (ggf. gemeinsamen) Verantwortlichkeit in Abgrenzung zur Auftragsverarbeitung, sofern Anbieter*in/Betreiber*in und Nutzer*in des Systems personenverschieden sind. Der gewählte Zweck hat zudem oftmals Auswirkungen auf die Wahl der Rechtsgrundlage. Ist die Erforderlichkeit der Datenverarbeitung Rechtmäßigkeitskriterium, ist diese Frage am jeweils verfolgten Verarbeitungszweck zu messen. Ebenfalls orientieren sich die Prinzipien der Datenminimierung, Speicherbegrenzung und Richtigkeit am Verarbeitungszweck. Der notwendige Detaillierungsgrad bei der Festlegung eines Zwecks steht wiederum in Wechselwirkung zum Risiko der Datenverarbeitung.

Zur praktischen Umsetzung bei KI-Systemen empfiehlt die DSK im Vorhinein die Erwartungen der verschiedenen Beteiligten bei der Nutzung von KI-Systemen zu spezifizieren (ggf. in einer maschinell zugänglichen Policy) sowie technische und organisatorische Maßnahmen zu etablieren, um Regelverstöße, Zweckdehnungen und Zweckverletzungen im Betrieb feststellen und dokumentieren zu können.[386]

5.4 Datenminimierung

Der Grundsatz der Datenminimierung basiert auf dem Gedanken, dass die Datenverarbeitung in Umfang und Eingriffsintensität auf das Maß begrenzt werden soll, welches für die Zweckerreichung wirklich erforderlich ist. Insgesamt sollten so wenig personenbezogene Daten wie möglich verarbeitet werden. Dieser Grundsatz kollidiert zwangsläufig mit adaptiven Lernverfahren, bei denen möglichst große Mengen an Daten verfügbar sein müssen.[387]

> **Art. 5 Abs. 1 Buchst. c DSGVO** Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein

5.4.1 Grundsatz

Besondere Erwähnung findet der Grundsatz der Datenminimierung im Rahmen der Regelungen zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Art. 25 DSGVO.[388] Die Zielsetzung des Konzepts „Privacy by Default & Design“ beschränkt sich allerdings nicht auf die Datenminimierung, sondern die Einhaltung aller in Art. 5 DSGVO niedergelegten Datenschutzprinzipien sowie dem Schutz der in Art. 1 Abs. 2 DSGVO genannten Grundrechte und Grundfreiheiten natürlicher Personen, d.h. insbesondere das in Art. 8 EU-GrCh niedergelegte Recht auf Schutz personenbezogener Daten aber auch die über Art. 7 EU-GrCh garantierte Achtung des Privat- und Familienlebens.[389]

---

[386] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 6.
[387] *Niemann/Kevekordes*, CR 2020, 17 (18); *Gausling*, DSRITB 2018, 519 (533).
[388] Vgl. *Grages/Plath*, CR 2017, 791 (796).
[389] *Baumgartner/Gausling*, ZD 2017, 308 (309).

5.4.2 Datenminimierung und Datenschutz durch Technikgestaltung

In Art. 25 DSGVO sind die Prinzipien „Privacy by Default & Design“ normiert. Das Prinzip der Datenminimierung kann schon dadurch umgesetzt werden, dass so wenig wie möglich personenbezogene Daten verarbeitet werden. Dies kann durch entsprechende Voreinstellungen in den Anwendungen erreicht werden. Des Weiteren kann das Prinzip der Datenminimierung durch Privacy by Design umgesetzt werden, indem schon im Entwicklungsprozess analysiert wird, welche Datenverarbeitung für einen Dienst notwendig und erforderlich sind und sich dementsprechend im Rahmen einer Anforderungsanalyse einer Dienst- oder Systementwicklung die notwendigen Daten und Datenverarbeitungsvorgänge identifizieren lassen. Da Art. 25 DSGVO sanktionsbewerte Vorgaben macht, soll im Folgenden analysiert werden, welche konkreten Anforderungen sich aus der Vorschrift unter besonderer Berücksichtigung der Kommunikation im Unternehmenskontext ableiten lassen.

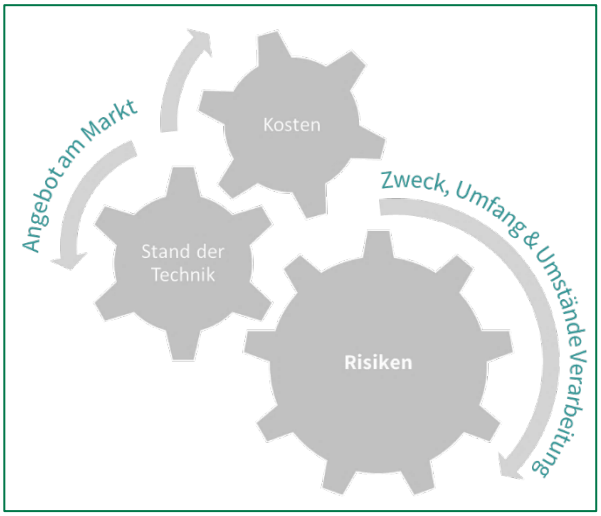
Adressat der Verpflichtung zum Privacy by Design/Default i.S.d. Art. 25 Abs. 1 und 2 DSGVO ist nur der Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO. Im Umkehrschluss bedeutet dies jedoch, dass die Hersteller von Produkten und Dienstleistungen nicht den Pflichten der Verordnung unterworfen sind. Die Vorstellung des Verordnungsgebers war, dass der Mechanismus des Privacy by Design „übers Dreieck“ wirken soll.[390] Dies wird weiterhin deutlich in ErwGr. 78:

> **Erwägungsrund 78 S. 4 DSGVO** In Bezug auf die Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten oder Produkten die entweder auf der Verarbeitung personenbezogener Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller […] ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

5.4.2.1 Umsetzung des risikobasierten Ansatzes

Art. 25 Abs. 1 DSGVO statuiert keine Pflicht besondere Technologien einzusetzen, sondern folgt dem technologieneutralen Ansatz der DSGVO.[391] Vielmehr sind unter Berücksichtigung der folgenden Aspekte „geeignete technische und organisatorische Maßnahmen“ als auch „die notwendigen Garantien“ umzusetzen, um den Anforderungen der DSGVO zu genügen:

- Stand der Technik,
- Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung sowie
- Unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.



[390] Vgl. *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 25 Rn. 25.
[391] Siehe ErwGr. 15 S. 1 DSGVO; vgl. auch VG Gelsenkirchen, Urt. v. 27.4.2020 – 20 K 6392/18 NVwZ-RR 2020, 1070 Rn. 64.

Je höher der Schutzbedarf und die Eingriffsintensität ausfällt, desto höhere Anstrengungen werden im Hinblick auf die zu ergreifenden Maßnahmen gestellt.[392] Spricht man von „KI-Systemen" so können ganz unterschiedlichste Anwendungen darunter fallen: von Sprachassistenten und Chat-Bots, automatischer Gesichtserkennung, Predicitve Policing, Deep-Fakes, bis hin zum autonomem Fahren. Diese Einsatzszenarien sind mit ganz unterschiedlichen Risikoprofilen verbunden.[393] Einen der zentralen Abwägungsfaktoren stellt dabei der Begriff des Risikos dar: Diese Formulierung entspricht dem risikobasierten Ansatz der DSGVO, welcher sich auch ganz maßgeblich in Art. 24, 32 und 35 DSGVO wiederspiegelt.[394] Entsprechend muss der verantwortliche eine Risikoanalyse in Form einer *systematischen und gründlichen Bewertung* der Verarbeitungstätigkeit durchführen, um Gegenmaßnahmen dem entsprechenden Risiko anzupassen.[395]

Abbildung 10 Risikobasierter Ansatz

Die Beurteilung in Art. 25 Abs. 1 DSGVO adressiert dabei zwei Zeitpunkte:

- zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch
- zum Zeitpunkt der eigentlichen Verarbeitung.

Insbesondere im Hinblick auf die Prägekraft der Technologie auf die soziale Welt im Sinne eines „*Code is Law*" ist in der Phase des Systemdesigns bereits zu bedenken, dass die späteren Entscheidungskorridore vorgezeichnet werden.[396] In dieser Norm manifestiert sich somit auch der *Vorfeldschutzcharakter* des Datenschutzrechts.[397] Dabei fordert der EDSA, dass Verantwortliche ihre Verarbeitungsvorgänge durch regelmäßige Überprüfungen der Wirksamkeit der von ihnen gewählten Maßnahmen und Sicherheitsvorkehrungen stets aktualisieren und neu bewerten.[398]

5.4.2.2 Ermittlung des Stands der Technik

Art. 25 Abs. 1 DSGVO verpflichtet zum Einsatz angemessener und „geeigneter" technischer und organisatorischer Maßnahmen (TOM) sowie „notwendiger" Schutzmaßnahmen („Garantien").[399] TOMs können in einem weiten Sinne als alle Methoden oder Mittel verstanden werden, die ein für die Verarbeitung Verantwortlicher einsetzen kann, um die Rechte und Freiheiten betroffener Personen zu schützen und die Grundsätze der DSGVO einzuhalten.[400] Die DSGVO verweist zwar vielfach auf den „Stand der Technik", enthält allerdings

[392] *Bieker*, DuD 2018, 27 (27).
[393] Siehe hierzu: *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 5 ff.
[394] *Baumgartner/Gausling*, ZD 2017, 308 (310). Zum risikobasierten Ansatz: *Bieker u. a.*, DuD 2018, 492 (492 f.); *Veil*, ZD 2015, 347 (347 ff.); *Schröder*, ZD 2019, 503; *Voigt,* in: Konzerndatenschutz Teil 3, Kapitel 2 Grundsätze der Verarbeitung nach der DSGVO, Rn. 14; *Martin u. a.*, DuD 2020, 149 (150 f.).
[395] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[396] *Wischmeyer*, AöR 2018, 1 (20 f.).
[397] Siehe zum Vorfeldschutz: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 89 ff.; vgl. auch *Bieker u. a.*, DuD 2018, 492 (492).
[398] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 11.
[399] Die DSGVO verwendet zwar in der deutschen Sprachfassung den Begriff „Garantien". Der Begriff „safeguards" der englischen Version, lässt sich inhaltlich allerdings besser mit Schutzvorkehrung oder Sicherungsmaßnahme übersetzen.
[400] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 6.

keine eigenständige Definition, sodass auf die in anderen Rechtskontexten entwickelten Grundsätze zurückgegriffen werden muss. [401] Da gerade im KI-Kontext viele Verfahren noch experimentell und Gegenstand von Forschung und Erprobung sind, stellt sich die Frage, auf welchen Erkenntnisstand rekurriert werden muss.

5.4.2.2.1 Abgrenzung „allgemein anerkannte Regeln der Technik“, „Stand der Technik“ und „Stand der Wissenschaft und Technik“

Auch wenn der Begriff nach Unionsrecht zu bestimmen ist, lohnt sich ein Blick auf die Begrifflichkeiten im deutschen Recht. Im Rahmen des deutschen Verfassungsrechts hat das BVerfG aufgezeigt, welcher Nuancierungen sich der Gesetzgeber bedienen kann, wenn rechtliche Anforderungen an aktuelle Entwicklungen aus der technischen Domäne geknüpft werden sollen: [402]

„Stand der Wissenschaft und Technik“	„Stand der Technik“	„Allgemein anerkannte Regeln der Technik“
Bei der Nutzung dieser Terminologie werden die vom Normadressaten zu berücksichtigenden Anforderungen „an die Front der technischen Entwicklung verlagert“. [403]	Ist zwischen den anderen beiden Technologieniveaus angesiedelt. [404] Der BGH verortet den Stand der Technik nicht in der Branchenüblichkeit, sofern der in der Branche praktizierte Standard hinter technisch Möglichem und rechtlich Gebotenen Standards zurückbleibt. [405] Normen und Standards, d.h. Regelungswerke von Standardisierungsgremien und internationalen Organisationen für Normung können als Indizien herangezogen werden. [406] Ist die technische Entwicklung über den Stand einer Norm hinausgegangen, reicht die Erfüllung der Norm hingegen nicht aus. [407]	Dieser Maßstab beschreibt die herrschende Auffassung unter den Praktiker*innen sowie bereits praktisch Bewährtes. Diese Regeln werden aber regelmäßig hinter weiterstrebenden, neueren technischen Entwicklungen hinterherhinken. [408]

5.4.2.2.2 Stand der Technik im Zivil- und Strafrecht

Eine weitere Annäherung an das Verständnis des Stands der Technik bietet ein vergleichender Blick auf die Verwendung der Begrifflichkeit in anderen Rechtsgebieten.

„Stand der Technik“ im Produkthaftungsrecht: § 1 Abs. 2 Nr. 5 ProdHaftG befreit den Hersteller eines Produkts i.S.d. § 2 ProdHaftG, wenn ein der Fehler i.S.d. § 3 Abs. 1 ProdHaftG nach dem „*Stand der Wissenschaft und Technik*“ in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. Ob ein Fehler vorliegt, hängt von den berechtigten Sicherheitserwartungen der in ei-

[401] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 8.
[402] BVerfGE 49, 89 (135 ff.) – Kalkar I.
[403] BVerfGE 49, 89 (135 ff.) – Kalkar I.
[404] *Bundesverband IT-Sicherheit e.V. (TeleTrusT),* Handreichung zum „Stand der Technik“, S. 11.
[405] BGHZ 181, 253 = NJW 2009, 2952 (2953); *Bräutigam/Klindt*, NJW 2015, 1137 (1141); *Schrader*, DAR 2016, 242 (243).
[406] BGH, Urteil vom 27.09.1994 - VI ZR 150/93, NJW 1994, 3349 (3350).
[407] BGH, Urteil vom 27.09.1994 - VI ZR 150/93, NJW 1994, 3349 (3350).
[408] BVerfGE 49, 89 (135 ff.) – Kalkar I.

nem bestimmten Bereich vorherrschenden Verkehrsauffassung im Zeitpunkt des Inverkehrbringens ab, welche wiederum daran anknüpfen, was objektiv wissenschaftlich-technisch möglich ist.[409] Der Stand der Wissenschaft und Technik bezeichnet den „Inbegriff der Sachkunde […], die im wissenschaftlichen und technischen Bereich vorhanden ist, also die Summe an Wissen und Technik, die allgemein anerkannt ist und allgemein zur Verfügung steht."[410] Um den aktuellen Stand festzustellen, kann oftmals auf Regelungswerke von Standardisierungsgremien und internationalen Organisationen für Normung (DIN, IEC, ISO) zurückgegriffen werden.[411] Da aber in den meisten Kontexten eine völlige Gefahrlosigkeit nicht erwartbar ist, orientiert sich der Maßstab grundsätzlich auch an der Bedeutung der gefährdeten Rechtsgüter und der Schadenseintrittswahrscheinlichkeit.[412] Je größer die Gefahren sind, desto höher fallen die Sicherheitserwartungen aus.[413] Im Hinblick auf den Haftungsausschluss kommt es nicht auf die individuellen Kenntnisse des Herstellers, sondern wieder wesentlich auf den Stand der Wissenschaft und Technik an.[414] Der Nachweis stellt recht hohe Anforderungen an das Qualitätsmanagement des Herstellers um zu beweisen, dass alle zum maßgeblichen Zeitpunkt verfügbaren Erkenntnisse ausgeschöpft wurden und die Gefährlichkeit des Produkts folglich von niemandem hätte erkannt werden können.[415]

„Stand der Technik" im Umweltschutzrecht: Eine Definition findet sich in § 3 Abs. 6 BImSchG. Danach beschreibt der Stand der Technik den „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme […] insgesamt gesichert erscheinen lässt".[416] Bei der Bestimmung des Standes der Technik sind insbesondere die in der Anlage zum BIMschG aufgeführten Kriterien zu berücksichtigen:

> Bei der Bestimmung des Standes der Technik sind unter Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen möglicher Maßnahmen sowie des Grundsatzes der Vorsorge und der Vorbeugung, jeweils bezogen auf Anlagen einer bestimmten Art, insbesondere folgende Kriterien zu berücksichtigen:
> 1. Einsatz abfallarmer Technologie,
> 2. Einsatz weniger gefährlicher Stoffe,
> 3. Förderung der Rückgewinnung und Wiederverwertung der bei den einzelnen Verfahren erzeugten und verwendeten Stoffe und gegebenenfalls der Abfälle,
> 4. vergleichbare Verfahren, Vorrichtungen und Betriebsmethoden, die mit Erfolg im Betrieb erprobt wurden,
> 5. Fortschritte in der Technologie und in den wissenschaftlichen Erkenntnissen,
> 6. Art, Auswirkungen und Menge der jeweiligen Emissionen,
> 7. Zeitpunkte der Inbetriebnahme der neuen oder der bestehenden Anlagen,
> 8. für die Einführung einer besseren verfügbaren Technik erforderliche Zeit,
> 9. Verbrauch an Rohstoffen und Art der bei den einzelnen Verfahren verwendeten Rohstoffe (einschließlich Wasser) sowie Energieeffizienz,
> 10. Notwendigkeit, die Gesamtwirkung der Emissionen und die Gefahren für den Menschen und die Umwelt so weit wie möglich zu vermeiden oder zu verringern,
> 11. Notwendigkeit, Unfällen vorzubeugen und deren Folgen für den Menschen und die Umwelt zu verringern,
> 12. Informationen, die von internationalen Organisationen veröffentlicht werden,
> 13. Informationen, die in BVT-Merkblättern enthalten sind.

„Stand der Technik" im Wettbewerbsrecht: Der österreichische Oberste Gerichtshof (ÖOGH) stellte

[409] BGH, Urteil vom 16.06.2009 - VI ZR 107/08, BGHZ 181, 253, NJW 2009, 2952 (2953); *Gomille*, JZ 2016, 76 (77); *Wagner,* in: MüKoBGB, § 1 ProdHaftG Rn. 50; *Seibl,* in: BeckOGK Zivilrecht, § 1 ProdHaftG Rn. 1222.
[410] *Seibl,* in: BeckOGK Zivilrecht, § 1 ProdHaftG Rn. 123; *Gomille*, JZ 2016, 76 (78).
[411] BGH, Urteil vom 27.09.1994 - VI ZR 150/93, NJW 1994, 3349 (3350).
[412] *Schrader*, DAR 2016, 242 (242 f.); *Gomille*, JZ 2016, 76 (77); *Bodungen, von/Hoffmann*, NZV 2018, 97 (98).
[413] BGH, Urteil vom 16.06.2009 - VI ZR 107/08, NJW 2009, 2952 (2953 f.), Rn. 18; *Horner/Kaulartz*, CR 2016, 7 (11).
[414] BT-Drs. 11/2447, S.15; *Schrader*, DAR 2016, 242 (243); *Wagner,* in: MüKoBGB, § 1 ProdHaftG Rn. 54.
[415] *Gomille*, JZ 2016, 76 (79); *Wagner/Goeble*, ZD 2017, 263 (266).
[416] *Moos,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 19 Rn. 39.

zum Stand der Technik fest, dass dieser sich einer einheitlichen Auslegung entzieht: so wird im Wettbewerbsrecht als „Stand der Technik“ einerseits das Fachwissen bezeichnet, über das der:die „Durchschnittsfachmann/-fachfrau“ auf dem betreffenden Gebiet verfügt (allgemein bekannt in Fachkreisen), – andererseits werden auch bestimmte Produkteigenschaften oder Herstellungsmethoden als zum „Stand der Technik“ gehörend bezeichnet. „Das schließt aber nicht aus, dass die dafür notwendigen Informationen im Sinn von Anleitungen oder Plänen geheim sein können, wenn sie der Fachmann nur mit erheblichem Aufwand entwickeln kann.“[417]

5.4.2.2.3 Definition des Europäischen Datenschutzausschusses (EDSA)

Der EDSA verortet in seinen Guidelines den "Stand der Technik" zwischen dem innovativeren Stand der "vorhandenen wissenschaftlichen Erkenntnisse und Forschung" und den etablierteren "allgemein anerkannten Regeln der Technik". Der "Stand der Technik" kann somit als das Technologieniveau einer Dienstleistung, Technologie oder eines Produkts identifiziert werden, das auf dem Markt existiert und am effektivsten ist, um die identifizierten Ziele zu erreichen. [418]

Abbildung 11 Abgrenzung der Technologiestände[419]

Technische Entwicklungen im Stadium des "Stands der Wissenschaft und Forschung" sind zumeist sehr dynamisch und gehen mit der Erreichung der Marktreife bzw. ihrer Markteinführung in das Stadium "Stand der Technik" über.[420]

5.4.2.3 Implementierungskosten

Unter den Implementierungskosten dürfen sowohl Anschaffungs- und Allgemeinkosten, Zeitressourcen sowie Personalkosten berücksichtigt werden.[421] Der Verantwortliche kann dabei das Verhältnis zwischen wirtschaftlichem Aufwand und praktischem Mehrwert für den Schutz der Daten miteinbeziehen.[422] Die Klärung, ob eine Maßnahme wirtschaftlich ist, erfordert eine individuelle Betrachtung des festgestellten Schutzbedarfs sowie der Realisierungskosten der erforderlichen Maßnahme.[423] Allerdings kann nach Einschätzung des EDSA ein Verweis auf zu hohe Kosten nicht von der Gewährleistung der Pflichten der DSGVO entbinden.[424]

[417] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f, Rn. 35; vgl. auch BGH, Urteil vom 22.3.2018 – I ZR 118/16, Rn. 35 ff.
[418] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 8.
[419] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 11.
[420] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 12.
[421] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[422] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 25 Rn. 22.
[423] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 10.
[424] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9; vgl. auch *Baumgartner/Gausling*, ZD 2017, 308 (310).

5.4.2.4 Art, Umfang, Umstände und Zwecke der Verarbeitung

Unter diesem Prüfungspunkt sind die Begleitumstände, Eigenschaften und Charakteristika einer geplanten Datenverarbeitung zu berücksichtigen, bspw.: [425]

- Werden besondere Kategorien personenbezogener Daten verarbeitet?
- Sind automatische Entscheidungsfindungen geplant?
- Besteht ein Machtungleichgewicht zwischen Verantwortlichem und betroffener Person?
- Sind Hürden für betroffene Personen bei der Rechtewahrnehmung zu befürchten?

Der Umfang stellt auf die Größenordnung und Reichweite der Verarbeitung ab, die Umstände betreffen sowohl den Verarbeitungskontext als auch die Erwartungen der betroffenen Personen, während sich der Zweck auf die Ziele der Verarbeitung bezieht. [426]

5.4.2.5 Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken

Je nach Einsatz-Szenario können KI-Systeme „in vielfältiger und teils nur schwer erkennbarer, vorhersehbarer oder beweisbarer Art und Weise Risiken für die Freiheiten und Rechte natürlicher Personen darstellen“.[427] Es bedarf daher eine auf KI zugeschnittene Art der Risikodefinition.

Methoden zur Ermittlung und Klassifizierung des in der DSGVO zentralen Begriffs des Risikos sind nicht unmittelbar in der DSGVO vorhanden. Entsprechend der in Art. 1 Abs. 2 DSGVO niedergelegten Ziele der DSGVO, stellt der Risikobegriff der DSGVO auf die Rechte und Freiheiten natürlicher Personen ab, welche insbesondere im Schutz der Grundrechte und Grundfreiheiten verankert sind.[428] Besonders relevant ist in diesem Zusammenhang das Recht auf Schutz personenbezogener Daten in Art. 8 EU-GrCh, aber auch der Schutz des Privatlebens in Art. 7 EU-GrCh, die Meinungsfreiheit in Art. 11 EU-GrCh, die Versammlungsfreiheit in Art. 12 EU-GrCh sowie das Diskriminierungsverbot in Art. 21 EU-GrCh können typischerweise durch die Verarbeitung personenbezogener Daten und die daraus resultierenden Folgen tangiert werden.[429] Welche Grundrechtspositionen im Einzelfall betroffen sind, hängt von der konkreten Verarbeitungssituation und ihrem Kontext ab. ErwGr. 75 DSGVO gibt weitere Hinweise, wie die Risikobeurteilung nach der DSGVO zu erfolgen hat:

> Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte […]

Beispiele: die Verarbeitung führt zu …

- einer Diskriminierung,
- einem Identitätsdiebstahl oder -betrug,
- einem finanziellen Verlust,

[425] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[426] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[427] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 5.
[428] *Bieker u. a.*, DuD 2018, 492 (492); *Bieker*, DuD 2018, 27 (27 f.); vgl. auch *Martin u. a.*, DuD 2020, 149 (150).
[429] *Bieker u. a.*, DuD 2018, 492 (492).

- einer Rufschädigung,
- einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- der unbefugten Aufhebung der Pseudonymisierung,
- anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann,
- wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht [bspw. Verzicht auf Ausübung ihrer Grundrechte[430]] oder
- daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
- wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden,
- wenn persönliche Aspekte bewertet werden, insbesondere
  - wenn Aspekte, welche die Arbeitsleistung,
  - wirtschaftliche Lage,
  - Gesundheit,
  - persönliche Vorlieben oder Interessen,
  - die Zuverlässigkeit oder das Verhalten
  - den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
- wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder
- wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Zusammenfassend ist nach der DSGVO ein Risiko stets dann anzunehmen, wenn die Möglichkeit besteht, dass ein Ereignis unmittelbar oder mittelbar zu einem Schaden für eine oder mehrere natürliche Personen führt.[431] Bereits ein *ungerechtfertigter* Eingriff in das Grundrecht einer natürlichen Person kann insofern als (immaterieller) Schaden gewertet werden – ungeachtet davon, ob daraus weitere materielle oder physische

DSK, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen

- „Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
- Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten."

[430] *Bieker u. a.*, DuD 2018, 492 (493).
[431] *DSK - Datenschutzkonferenz*, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen, S. 1; *Martin u. a.*, DuD 2020, 149 (150 f).

Schäden resultieren.[432]

Schwierigkeiten bereitet die Risikobeurteilung, wenn konstatiert wird, dass die vom Verantwortlichen anzustellende Bewertung „in Worte gefasst" werden kann, aber „nicht in sinnvoller Weise zahlenmäßig quantifiziert werden kann."[433] Insofern gilt auch zu bedenken, dass das klassische Risikomanagement zumeist Risiken aus Perspektive der Organisation (und nicht der betroffenen Person) betrachtet und zudem oftmals eher von „greifbaren" materiellen oder physischen Schäden ausgeht.[434] Vorgeschlagen wird zur Herstellung einer Vergleich- und Überprüfbarkeit die Einteilung in Kategorien, d.h. die stufenweise Kategorisierung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden bspw. in die Risikokategorien gering – normal – hoch.[435] Jede durchschnittliche Datenverarbeitung wäre als „normal" einzustufen, sodass das Prädikat „gering" den Einsatz geeigneter TOMs impliziere.[436] Für den Verantwortlichen wäre der in Abbildung 12 dargestellte Prozess zu durchlaufen.

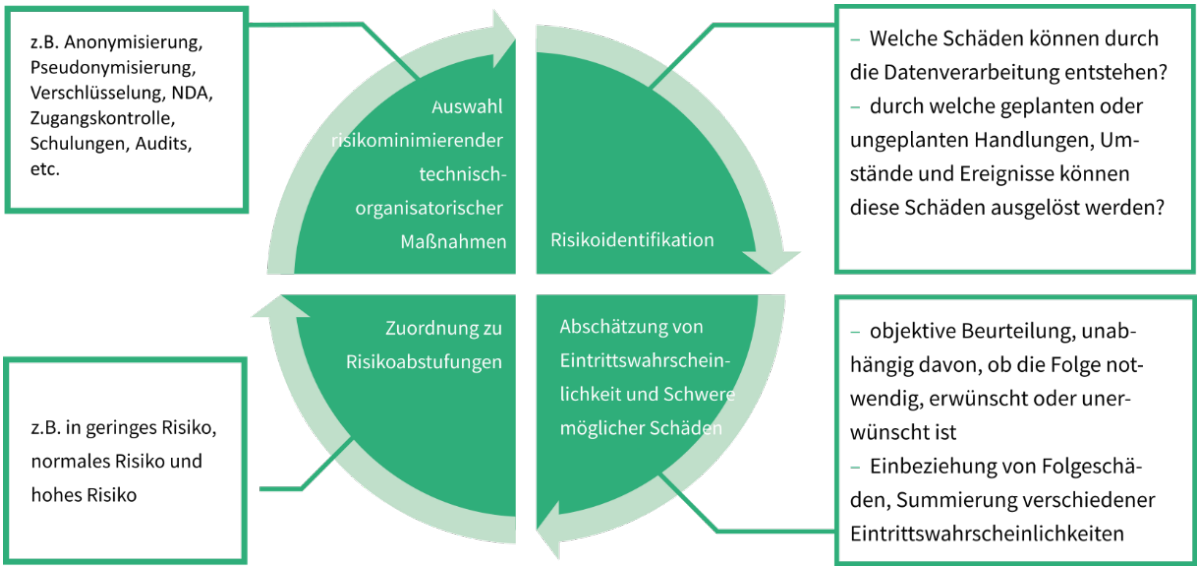


Abbildung 12 Risikobeurteilung

Bei der Feststellung eines hohen Risikos ist eine Datenschutz-Folgenabschätzung durchzuführen (siehe Abschnitt 5.4.2.1). Bezüglich der potentiell schadensauslösenden Ereignisse wird darauf hingewiesen, dass neben den geplanten Verarbeitungsfolgen auch unbeabsichtigte Negativfolgen, die durch Abweichungen vom „Best-Case-Szenario" entstehen könnten, berücksichtigt werden sollten.[437] Bei der Identifikation der Risikoquellen sollten anders als in der IT-Sicherheit bei der Angreifermodellierung nicht nur aus Sicht des Verantwortlichen potentielle Angriffe „von außen" antizipiert werden, sondern aus Sicht der betroffenen Person

[432] *Bieker u. a.*, DuD 2018, 492 (493); *Martin u. a.*, DuD 2020, 149 (151). Wichtig zu bedenken ist hierbei, dass nicht bereits mit jedem Eingriff in Art. 8 Abs. 1 EU-GrCh, d.h. jeder rechtfertigungsbedürftigen Verarbeitung personenbezogener Daten ein Risiko i.S.d. Art. 25 Abs. 1 DSGVO vorliegen kann: *Veil*, NVwZ 2018, 686 (694); *Bieker*, DuD 2018, 27 (29); *Magiera*, DÖV 2000, 1017 (1022); *Wagner*, Datenökonomie und Selbstdatenschutz, S. 233.

[433] *Bieker u. a.*, DuD 2018, 492 (493).

[434] *Martin u. a.*, DuD 2020, 149 (151); *Schiering u. a.*, DuD 2020, 161 (162). In diesem Sinne sollte nicht von „Angreifern" als Risiko-Quelle gesprochen werden, da Risikoauslöser auch interner Natur, wie die eigenen Beschäftigten sein können. „Beteiligte" oder „beteiligte Akteure" werden als neutrale Begriffe vorgeschlagen, in: *Schiering u. a.*, DuD 2020, 161 (162).

[435] *Bieker u. a.*, DuD 2018, 492 (493).

[436] *Bieker u. a.*, DuD 2018, 492 (493).

[437] *Bieker u. a.*, DuD 2018, 492 (493).

ausgehend jegliche Risikoquelle zu bedenken, welche anhand von Schutzzielen klassifiziert werden könnten.[438]

5.4.2.5.1 KI-spezifische Risiken und Abhilfemaßnahmen

Die Gestaltung „intelligenter" Datenverarbeitungssysteme hat entscheidenden Einfluss auf das Risiko für die Rechte und Freiheiten der betroffenen Personen.

Nachvollziehbarkeit: Je leichter der Dateneinsatz bspw. über Dokumentation, Protokolle und Tests nachvollziehbar ist, desto eher ist die Rechtmäßigkeit der Verarbeitungstätigkeit überprüfbar. Insbesondere hängt mit den Einblicken in das Systemdesign auch die Möglichkeit der Verhinderung verdeckter Diskriminierung zusammen.[439] Bei gleichwertigen Alternativen seien laut Positionierung der DSK daher solche Systeme zu bevorzugen, die einem menschlichen Verständnis zugänglich sind (wie bspw. einfacher nachvollziehbare Modelle wie Regressionsmodelle oder Entscheidungsbäume). [440] Zudem sollten für unterschiedliche Zielgruppen (Verantwortliche, Betroffene, Aufsichtsbehörden) unterschiedliche Level an Transparenz erforderlich.[441] Über ein Verifikationsmodell ließe sich die Güte des Systems beurteilen und Betroffenen sollten Fehlerbestimmung und Fehlermaß transparent gemacht werden. Zur Annäherung der Erklärbarkeit komplexer Systeme könnten Eigenschaften von KI-Komponenten mit Black-Box-Tests untersucht werden, wobei mit Hilfe von synthetischen Testdaten geprüft wird, welchen Einfluss die Eingabeparameter auf die Ausgabe der KI-Komponente haben. [442]

Vorhersehbarkeit: Mit nicht-deterministischen, im laufenden Betrieb weiterlernenden adaptiven Systemen steigt das Risiko unvorhergesehener Fehlentscheidungen, sodass die DSK fordert bei vergleichbarer Effizienz und Effektivität deterministische Systeme zu verwenden.[443] Liegt die Leistungsfähigkeit des nicht-deterministischen Systems hingegen höher, so könne dieses nach sorgfältiger Abwägung der Risiken zum Einsatz kommen, sofern die Leistungsüberlegenheit quantitativ dargelegt werden kann. [444] Andere wiederum schlagen fortlaufende Kontrollen mit ebenfalls intelligenten Prüfwerkzeugen, wie Kontrollalgorithmen vor, welche die Entscheidungsergebnisse systematisch analysieren, sowie die kontinuierliche Prüfung der Trainingsumgebung, Validität der Testdaten und Richtigkeit der Datenbasis.[445]

Eingriffsmöglichkeiten: Um Systeme vor schädlichen Einflüssen zu schützen, sollte sichergestellt sein, dass es nur durch Befugte konzipiert, programmiert, trainiert, genutzt und überwacht wird und auch nur

[438] *Bieker u. a.*, DuD 2018, 492 (494).
[439] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 5 f.
[440] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 6.
[441] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 12.
[442] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 12; *Gausling*, DSRITB 2018, 519 (536).
[443] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 6.
[444] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 6.
[445] *Martini*, JZ 2017, 1017 (1022).

diese die Möglichkeit zum Eingreifen in die Verarbeitung haben. [446] Gleichzeitig können Interventionsmechanismen genutzt werden, um Falsch-Positiv und Falsch-Negativ-Klassifikationen frühzeitig zu detektieren.[447]

Datenqualität: Die Aufbereitung von Rohdaten zu Trainingsdaten im Hinblick auf Relevanz, Qualität, Integrität, Repräsentativität und Heterogenität sowie die Aufteilung in Trainings-, Validierungs- und Testdaten sind wesentliche Schritte in der Phase des Systemdesigns. [448] Lückenhafte oder verzerrte Daten führen regelmäßig zu Fehlentscheidungen.[449] Insofern kommt es wiederum zu einer Rückbesinnung auf den Zweck des KI-Systems für die Datenauswahl. Bezüglich der Transparenz fordert die DSK zudem die Ausweisung der Herkunft der Rohdaten, sowie ob und wer Daten „veredelt" hat.[450] Flankierende Sicherheitsmaßnahmen in der gesamten Verarbeitungs- und Übermittlungskette senken das Risiko, dass Roh- und Trainingsdaten unbefugt verändert wurden. [451]

Datenmenge: Rohdaten sollten nach Ansicht der DSK auf wenige, inhaltlich gut verstandene Dimensionen reduziert werden.[452] Dabei sollten sehr hoch korrelierende Daten, d. h. solche Daten, die in einer engen Wechselbeziehung stehen, verwendet werden und das Korrelationsmaß nachgewiesen. Eine zu einseitig verstandene, nicht ausgewogene Minimierung von Daten kann aber die Integrität der Modellierung von KI-Systemen gefährden. [453] Bei der Wahl der Datenkategorien sollte auf die Diskriminierungsneigung geachtet werden. Diese kann auch bei Ersatzvariablen vorliegen, da stark korrelierende Daten ebenfalls hohes Diskriminierungspotential enthalten können (soll bspw. das Geschlecht bei einer KI-basierten Entscheidung nicht berücksichtigt werden, ergibt sich dies zumeist dennoch aus dem Vornamen).[454]

Nichtverkettung: Über die Erkennung von Mustern und Korrelationen sind KI-Systeme für die Verkettung unterschiedlicher Erkenntnisse aus „unverdächtigen" Daten geeignet.[455] Problematisch ist es, wenn diese Ergebnisse nicht vom Ursprungszweck gedeckt sind.[456]

De-Anonymisierung: KI-Systeme können Erkenntnisse und Zwischenergebnisse generieren, die (auch ungewollt) eine Identifizierung von Personen ermöglichen und u.U. sensible Rückschlüsse auf Personen ermöglichen.[457] Es sollte technisch sichergestellt werden, dass diese (Zwischen-)Ergebnisse nicht langfristig gespeichert werden und nur ein fest definierter Personenkreis zu vorher festgelegten Zwecken, protokolliert Zugriff auf diese Zwischenergebnisse hat.[458]

---

[446] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 7.
[447] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 14.
[448] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 7, 10.
[449] *Wischmeyer*, AöR 2018, 1 (23).
[450] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 8.
[451] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 8.
[452] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 9.
[453] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 9.
[454] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 9.
[455] Vgl. zum Zusammenhang mit der Diskussion um „Big Data": *Schefzig*, DSRITB 2018, 491 (497) m.w.N.
[456] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 14.
[457] *Niemann/Kevekordes*, CR 2020, 17 (18 f.); *Schefzig*, DSRITB 2018, 491 (497).
[458] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 15.

Als Bausteine der Risikominimierung lassen sich zusammenfassen:

5.4.2.5.2 Modelle zur Operationalisierung der Anforderungen der DSGVO

Mit dem Standard-Datenschutzmodell (SDM)[459] sollen Anforderungen der DSGVO für den Verantwortlichen leichter handhabbar werden und so eine rechtskonforme und überprüfbare Umsetzung erreichbar sein, u.a. durch eine objektive und überprüfbare Beurteilung eines Verfahrens.[460] Das SDM besteht aus mehreren Bausteinen, u.a. zum Aufbewahren, Dokumentieren, Löschen und Vernichten und Berichtigen. Diese sollen rechtliche Anforderungen in konkrete technische und organisatorische Maßnahmen „übersetzen".[461] Die aktuellen Bausteine sind auf Seiten der Landesbehörden abrufbar.[462]

Das Modell orientiert sich dabei an den Gewährleistungszielen der Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.[463] Diese Ziele sollen die Modellierung von funktionalen Anforderungen in praktischen Anwendungsfällen vereinfachen und die einfache Visualisierung von Konflikten unterstützen. Sie werden auch als „Optimierungsgebote" gefasst.[464] Die technische Gestaltung von Verarbeitungstätigkeiten sollte sich an diesen Zielen orientieren und auf diese Weise die rechtlichen Anforderungen der DSGVO in technische und organisatorische Maßnahmen transferieren.[465] Für die unterschiedlichen technischen Komponenten (Daten, Systeme, Dienste, Prozesse) beschreibt das SDM

[459] Zum Standard-Datenschutzmodell: https://www.datenschutzzentrum.de/sdm/ [letzter Abruf 20.07.2021].
[460] *Bieker*, DuD 2018, 27 (27).
[461] Vgl. BfDI, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html [letzter Abruf 18.08.2021].
[462] Siehe: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ [letzter Abruf 18.08.2021].
[463] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 10, abrufbar unter: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf [letzter Abruf 18.08.2021].
[464] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 9.
[465] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 25 ff.

mit seinen Bausteinen Referenzmaßnahmen, die sich systematisch an den Gewährleistungszielen orientieren und so eine strukturierte Umsetzung in der Praxis befördern sollen. Dabei muss stets bedacht werden, dass ein Datenschutzmanagementprozess ein zyklischer Prozess ist.[466] Dies bedeutet, es sind regelmäßige Überprüfungen der Wirksamkeit der Maßnahmen erforderlich.

5.4.2.5.3 Schutzstufenkonzept

Um neben der Eintrittswahrscheinlichkeit die Schwere eines möglichen Schadens zu bemessen, können personenbezogene Daten in unterschiedliche Schutzstufen eingeordnet werden. Eine solche Klassifizierung erleichtert die Einschätzung der Sensitivität bestimmter Daten, muss im Rahmen der Gefahren- und Risikoanalyse zur Auswahl geeigneter TOMs gemeinsam mit den entsprechenden Eintrittswahrscheinlichkeiten betrachtet werden.

Stufe	Personenbezogene Daten	Beispiele	Schwere eines möglichen Schadens
A	Daten wurden von betroffenen Personen frei zugänglich gemacht	Telefonverzeichnis, eigene frei zugänglich gemachte Webseite	geringfügig
B	Daten wurden nicht frei zugänglich gemacht, aber eine besondere Beeinträchtigung ist bei unsachgemäßer Handhabung nicht zu erwarten	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	
C	Unsachgemäße Handhabung dieser Daten können betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen („Ansehen“)	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	Unsachgemäße Handhabung dieser Daten können betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen *erheblich* beeinträchtigen („Existenz“)	Arbeitszeugnisse, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Anstaltsunterbringung, Straffälligkeit, sonstige Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell
E	Unsachgemäße Handhabung dieser Daten können Gesundheit, Leben oder Freiheit der betroffenen Person beeinträchtigen	Daten über mögliche Opfer einer Straftat, Zeugenschutzprogramm	groß

[466] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 31.

Tabelle 2 Niedersächsisches Schutzstufenkonzept der LfD Niedersachsen[467]

5.4.3 Datenminimierung und datenschutzfreundliche Voreinstellungen

Diese Vorgabe des Art. 25 Abs. 2 DSGVO trägt dem Umstand Rechnung, dass Nutzende datenverarbeitender Systeme oftmals die voreingestellten Werkseinstellungen nicht maßgeblich verändern.[468] Um die Ziele der Datenminimierung auch effektiv umzusetzen, sind Verantwortliche angehalten, Voreinstellungen so wählen, dass nur für den jeweils bestimmten Verarbeitungszweck erforderliche Daten erhoben werden, d.h. im Hinblick auf Menge der personenbezogenen Daten, den Umfang der Verarbeitung dieser Daten, der Speicherdauer sowie der Zugänglichkeit nur das entsprechend der einschlägigen Legitimationsgrundlage nach Art. 6 Abs. 1 DSGVO zwingend erforderliche Minimum vorgesehen werden soll.[469]

5.4.4 Die Datenschutz-Folgenabschätzung als Ausfluss des risikobasierten Ansatzes

Wird im Rahmen der Risikobeurteilung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen festgestellt, muss eine Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO durchgeführt werden. Insofern sind Verarbeitungskonzepte nicht per se verboten, sondern es wird eine Struktur forciert, die eine umfassenden, vollständige und kontinuierliche Identifikation, Bewertung sowie Eindämmung und Überwachung der Risiken gewährleisten soll.[470] Erst wenn im Rahmen der DSFA keine risikominimierenden Maßnahmen umsetzbar erscheinen und das Risiko weiterhin hoch bleibt, muss die zuständige Aufsichtsbehörde nach Art. 36 DSGVO konsultiert werden.

5.4.4.1 Notwendigkeit der DSFA

Eine gesetzliche Pflicht zur Durchführung einer DSFA besteht, wenn die geplante Datenverarbeitung voraussichtlich ein *hohes Risiko* für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Insofern sollte es für einen umfassenden Schutz ausreichen, wenn ein Teilbereich besonders risikobehaftet ist – selbst wenn dies nicht für den gesamten Verarbeitungsvorgang gelten mag.[471] Bezüglich der geschützten „Rechte und Freiheiten“ gelten die gleichen Erwägungen wie bei Art. 25 DSGVO (Privacy by Design, Abschnitt 5.4.2.5). Zudem nennt Art. 35 Abs. 3 DSGVO Beispiele, in denen stets von der Erforderlichkeit einer DSFA auszugehen ist.

- Entscheidungen mit Rechtswirkung oder erheblicher Beeinträchtigung auf Basis systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen durch *automatisierte* Verarbeitung, einschließlich Profiling,
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder Daten über strafrechtliche Verurteilungen und Straftaten,
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

[467] Die Landesbeauftragte für den Datenschutz Niedersachsen, Schutzstufenkonzept der LfD Niedersachsen, Stand: Oktober 2018, abrufbar unter: https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/schutzstufen/schutzstufen-56140.html [letzter Abruf 13.08.2021].
[468] *Baumgartner/Gausling*, ZD 2017, 308 (312).
[469] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 11.
[470] *Bieker u. a.*, DuD 2018, 492 (494 f.); *Martin u. a.*, DuD 2020, 149 (153); *Schiering u. a.*, DuD 2020, 161 (162).
[471] *Martin u. a.*, DuD 2020, 149 (150).

Art. 35 Abs. 4 und 5 DSGVO ermöglichen es ferner den Aufsichtsbehörden Positiv- und Negativlisten aufzustellen und somit Fälle zu benennen, in denen die DSFA stets notwendig ist oder nicht notwendig ist. Die DSK hat eine solche nicht-abschließende Liste erstellt.[472] In allen übrigen Fällen ist mithilfe einer Risikoabschätzung eine Schwellwertanalyse durchzuführen.[473] Die Artikel-29-Datenschutzgruppe hat auf Grundlage von Art. 35 und ErwGr. 71, 75 sowie 91 DSGVO neun Kriterien entwickelt, anhand derer sich beurteilen lässt, ob voraussichtlich ein hohes Risiko besteht:[474]

1. Verarbeitungen, die Verhalten bewerten oder einstufen, u.a. Erstellen von Profilen und Prognosen
2. automatisierte Entscheidungen mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. systematischer Überwachung
4. vertrauliche oder höchstpersönliche Daten
5. Verarbeitung von Daten in großem Umfang, zu messen anhand:
   - Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
   - verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
   - Dauer oder Dauerhaftigkeit der Datenverarbeitung;
   - geografisches Ausmaß der Datenverarbeitung
6. Abgleichen oder Zusammenführen von Datensätzen aus verschiedenen Quellen, die zu unterschiedlichen Zwecken erhoben wurden oder von unterschiedlichen Verantwortlichen stammen, in einer Weise, die über die vernünftigen Erwartungen der betroffenen Personen hinausgehen
7. Daten zu schutzbedürftigen Betroffenen und bei Machtungleichgewichten, wie bspw. bei Kindern, Beschäftigten, Teilen der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber*innen, Senior*innen, Patient*innen usw.) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen vorliegt
8. innovative Nutzungen oder die Anwendung neuer technologischer oder organisatorischer Lösungen (z.B. Fingerabdruck- und Gesichtserkennung für die Zugangskontrolle)
9. Fälle, in denen die Verarbeitung die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages hindert (z.B. Auskunfteien)

Ein hohes Risiko ist stets dann zu erwarten, wenn zwei oder mehr Kriterien gegeben sind. Hohe Risiken können aber auch vorliegen, wenn nur eines oder keines der Kriterien erfüllt sind – insofern kommt es immer auf eine Betrachtung des Einzelfalls an.[475] Da KI als neue Technologie zu qualifizieren ist, wird regelmäßig eine DSFA erforderlich sein.[476]

---

[472] DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, abrufbar unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf [letzter Abruf 21.07.2021].

[473] *Bieker u. a.*, DuD 2018, 492 (495).

[474] *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" - WP248 Rev.01, S. 10 ff.

[475] *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" - WP248 Rev.01, S. 12.

[476] *Schürmann*, ZD 2022, 316.

5.4.4.2 Durchführung der DSFA

Art. 35 Abs. 7 DSGVO umschreibt die Umsetzung der DSFA. Die wichtigsten Elemente zeigt Abbildung 13. Eine ausführlichere Beschreibung einzelner Schritte dieses iterativen Prozesses kann Abbildung 14 entnommen werden.

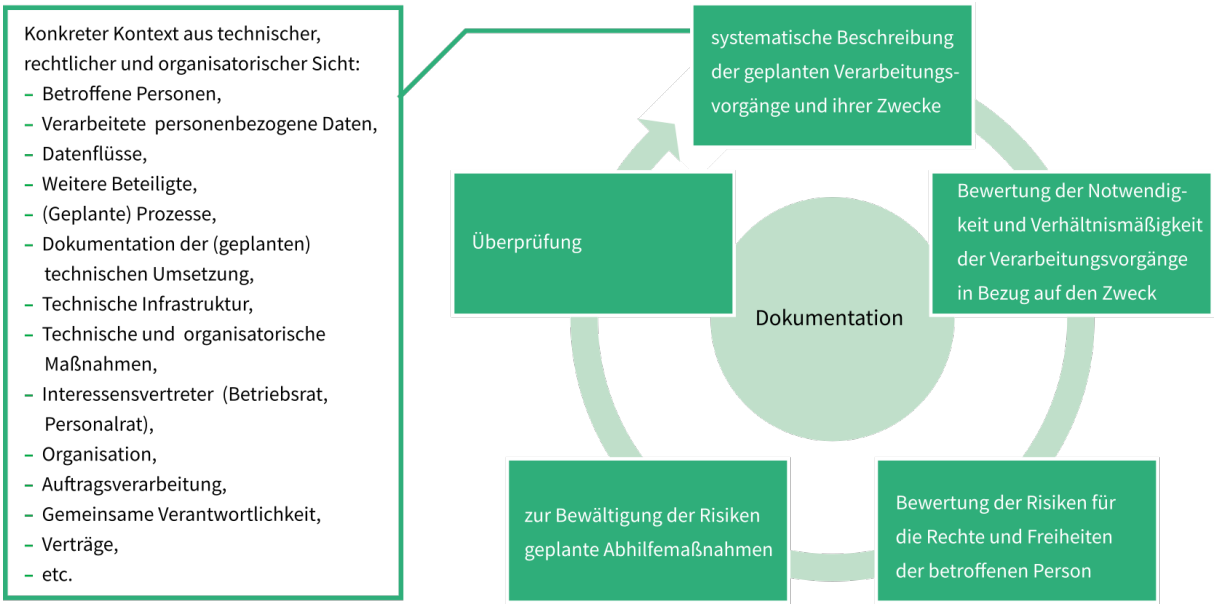


Abbildung 13 Durchführung einer DSFA gemäß Art. 35 Abs. 7, 11 DSGVO

Rollen & Verantwortlichkeit: In organisatorischer Hinsicht nimmt die Rolle des:der Datenschutzbeauftragten eine bedeutende Position ein: sie hat gemäß Art. 35 Abs. 2 und Art. 39 Abs. 1 Buchst. c DSGVO die Durchführung der DSFA zu überwachen und den Verantwortlichen zu beraten. Der EDSA betont dabei, dass es Aufgabe des Verantwortlichen ist die DSFA durchzuführen.[477] Datenschutzbeauftragte können ihrer Überwachungsfunktion nicht gerecht werden, wenn die Aufgabe der DSFA an sie delegiert wird.[478] Sowohl der Rat des Datenschutzbeauftragten als auch Begründungen für Abweichungen von diesem Rat, sollten schriftlich dokumentiert werden.[479] Erfolgt die Datenverarbeitung durch einen Auftragsverarbeiter, muss dieser bei der DSFA-Durchführung unterstützen (Art. 28 Abs. 3 Buchst. f DSGVO). Bei gemeinsam für die Verarbeitung Verantwortlichen müssen deren jeweilige Aufgaben genau festgelegt werden und in ihrer DSFA hinterlegt sein, welcher Verantwortliche für die verschiedenen Maßnahmen zuständig ist, mit denen die Risiken mitigiert werden. [480]

Hersteller von Systemen oder Komponenten sind hingegen nicht verpflichtet, eine DSFA durchzuführen, da

[477] *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" - WP248 Rev.01, S. 17; *Martin u. a.*, DuD 2020, 149 (151).
[478] *Martin u. a.*, DuD 2020, 149 (151).
[479] *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" - WP248 Rev.01, S. 18.
[480] *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" - WP248 Rev.01, S. 8.

sie keine Verantwortlichen sind, sofern sie nicht in Datenverarbeitungsvorgänge eingebunden sind. Sie könnten allerdings eine generische DSFA für ihre Produkte erstellen und ihren Kundschaft bereitstellen.[481] Von Vorteil wäre, dass sie sich am besten mit der Technologie auskennen – gleichzeitig bestehen Nachteile, wenn der spätere Anwendungskontext nicht ausreichend überblickt wird, und somit eine sinnvolle Risikoanalyse kaum möglich ist.[482] Da eine DSFA zum Ziel hat systematisch neue Situationen zu untersuchen, kann eine DSFA für bereits untersuchte Fälle (d.h. für in einem bestimmten Zusammenhang und zu einem bestimmten Zweck durchgeführte Verarbeitungsvorgänge) nicht mehr notwendig sein.[483] Dies wäre der Fall bei:

- Erfassung derselben Art von Daten
- Verarbeitung zum gleichen Zweck
- Einsatz einer ähnlichen Technologie

Daraus folgt, dass eine Referenz-DSFA zur Nutzung durch mehrere Verantwortliche durchaus möglich ist. Für den Verantwortlichen verbleibt zwar die Pflicht eine DSFA vorweisen zu können, es dürfen hierfür aber Referenz-DSFAs und Angaben aus einer vom Produktlieferanten erstellten DSFA verwendet werden. [484]

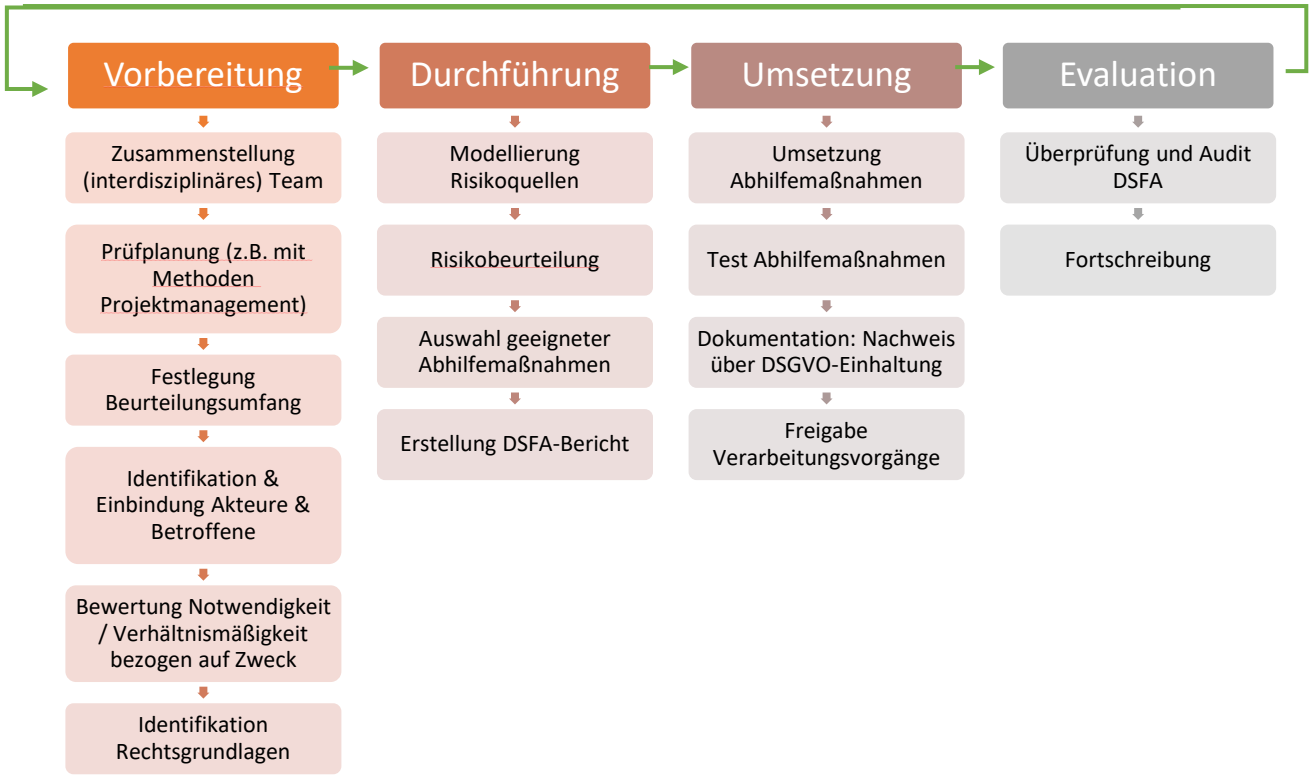


Abbildung 14 Bestandteile eines iterativen Prozesses der DSFA nach DSK[485]

[481] *Martin u. a.*, DuD 2020, 149 (151).
[482] *Martin u. a.*, DuD 2020, 149 (151).
[483] *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" - WP248 Rev.01, S. 8.
[484] *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" - WP248 Rev.01, S. 8.
[485] *DSK - Datenschutzkonferenz*, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.

Prozessschritte: Nachdem das idealerweise interdisziplinär entsprechend der betroffenen Fachbereiche besetzte Team zur Durchführung der DSFA zusammengestellt wurde und das weitere Vorgehen in einem Prüfplan festgehalten ist, müssen zur Ermittlung des Beurteilungsspielraums die Verarbeitungsvorgänge und Datenflüsse beschrieben und von anderen (Geschäfts-)Prozessen abgegrenzt werden.[486] Bei der Einbindung relevanter Akteure kann auch die Einbindung des Betriebsrats als Arbeitnehmervertretung angezeigt sein. Sodann sind die zuvor identifizierten und systematisch beschriebenen Datenverarbeitungsvorgänge auf ihre Notwendigkeit und Verhältnismäßigkeit sowie das Vorliegen einer Rechtsgrundlage zu prüfen. Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen zunächst umfassend identifiziert und anschließend bewertet werden. Zur Eindämmung dieser Risiken erfolgt eine Auswahl geeigneter Abhilfemaßnahmen, die anschließend umgesetzt werden. Verbleibende Restrisiken sind zu ermitteln und zu dokumentieren. Insgesamt sind die Ergebnisse in einem Bericht zusammenzustellen. Die DSFA ist an dieser Stelle allerdings noch nicht beendet, sondern sollte als iterativer Prozess auch die Umsetzungsphase umfassen: Denn sollte sich bei der Umsetzung herausstellen, dass geplante Maßnahmen nicht wie geplant wirken oder überhaupt nicht realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden. Insofern ist auch der Test der Abhilfemaßnahmen relevant. Spätestens wenn sich das mit der Verarbeitung verbundene Risiko ändert, muss erneut eine DSFA durchgeführt werden.

5.4.4.3 Ergebnis der DSFA

Im Idealfall führt das Ergebnis der DSFA dazu, dass das Risiko erfolgreich mitigiert wurde. Gleichzeitig verbleibt die Notwendigkeit, dies regelmäßig zu überprüfen, und bei Bedarf die DSFA neu zu starten. Konnte das Risiko hingegen nicht ausreichend abgesenkt werden, ist die Aufsichtsbehörde zu konsultieren.

Konsultation Aufsichtsbehörde: Können Abhilfemaßnahmen das Risiko nicht ausreichend senken (hohes Restrisiko) und will der Verantwortliche an der geplanten Datenverarbeitung festhalten, ist eine vorherige Konsultation bei der Aufsichtsbehörde durchzuführen. Die Behörde ist gemäß Art. 36 Abs. 2 DSGVO verpflichtet, innerhalb von 8 Wochen eine schriftliche Empfehlung zu unterbreiten, und kann ihre in Art. 58 DSGVO genannten Befugnisse ausüben.

Kontinuierlicher Prozess: Art. 35 Abs. 11 DSGVO zeigt, dass es sich bei der DSFA nicht um einen einmaligen, linearen Prozess handelt, sondern regelmäßige Überprüfungen der Restrisiken sowie der Umsetzung der DSFA während des gesamten Lebenszyklus der Verarbeitungsvorgänge als auch eine erneute Durchführung der DSFA erforderlich sind, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind. Insbesondere bei im Betrieb weiter-/selbstlernenden KI-Systemen muss regelmäßig überprüft werden, ob es durch neuen Input zu verändertem Output kommt, und ob sich damit die Risiken für betroffene Personen verändern.[487]

Dokumentation: Selbst wenn der Verantwortliche eine DSFA nicht für erforderlich hält, sollte diese Entscheidung schriftlich begründet und dokumentiert werden. [488] Dies reiht sich in die sonstigen Dokumentationspflichten ein: so ist das Führen eines Verzeichnisses von Verarbeitungsvorgängen gemäß Art. 30 Abs. 1 DSGVO (abgesehen von den Ausnahmenfällen des Art. 30 Abs. 5 DSGVO) ohnehin stets erforderlich.

---

[486] *DSK - Datenschutzkonferenz*, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, S. 2.
[487] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 18.
[488] *Bieker u. a.*, DuD 2018, 492 (495).

Praxistipp

(1) Wer neuartige KI-Werkzeuge einzusetzen plant, sollte eine DSFA durchführen.
(2) Anbieter von KI-Werkzeugen müssen bei der Durchführung unterstützen, wenn sie als gemeinsam Verantwortliche oder Auftragsverarbeiter an der Verarbeitung personenbezogener Daten beteiligt sind.
(3) Anbieter von KI-Lösungen, die an der Datenverarbeitung nicht beteiligt sind, können ihr Angebot nichtsdestotrotz um eine Muster-DSFA erweitern, in denen eine systematische Beschreibung der Verarbeitungsvorgänge und technischen Parameter bereits erarbeitet ist, sodass Anwender*innen lediglich die konkrete Umsetzung berücksichtigen müssen.
(4) Dokumentation der Risikobeurteilung, inklusive:
   a. Dokumentation der Entscheidung für/gegen die Durchführung der DSFA (mit Begründung).
   b. Kam es zu einer Fehleinschätzung, kann es Einfluss auf potentielle Sanktionen haben, ob diese auf einer nachprüfbaren Begründung basiert.

5.4.5 Zwischenergebnis zur Datenminimierung sowie der Umsetzung des risikobasierten Schutzkonzepts

Eine der zentralen Weichenstellungen innerhalb des modernen Datenschutzrechts ist die Ermittlung des konkreten Risikos einer geplanten Verarbeitung personenbezogener Daten für die betroffene(n) Person(en) und die Minimierung dieses Risikos durch die Auswahl geeigneter Schutzmaßnahmen technischer oder organisatorischer Natur (TOMs).

Je weniger personenbezogene Daten für die Umsetzung des KI-Systems verarbeitet werden müssen, desto geringer fallen die Risiken aus. Des Weiteren ist entscheidend, ob es sich um automatisierte Entscheidungen handelt, oder bloße Assistenzsysteme, welche eine menschliche Letztentscheidung lediglich vorbereitet, sofern hier tatsächlich noch eine inhaltliche Überprüfung stattfindet.[489] Dies hat auch zur Folge: je geringer die Risiken durch das technische Systemdesign bereits sind, desto weniger Pflichten treffen die für den Einsatz verantwortliche Stelle, weitere Maßnahmen zu ergreifen. So entfällt bspw. die Pflicht eine DSFA durchzuführen, wenn mit der Datenverarbeitung kein hohes Risiko verbunden ist. Bietet der KI-Einsatz hingegen immer detailliertere Tiefenanalysen, ist aller Voraussicht nach eine DSFA erforderlich und sollte als Compliance-Tool frühzeitig eingesetzt und regelmäßig wiederholt werden, um negative Folgen, wie bspw. die Fortentwicklung selbstlernender Algorithmen zu diskriminierenden Systemen, effektiv entgegenzuwirken.[490]

Den Verantwortlichen treffen folgende Pflichten:

- Beurteilung des für die betroffenen Personen mit der Datenverarbeitung verbundenen Risikos: Analyse der Datenschutzfreundlichkeit der Technikgestaltung und Voreinstellungen
- Bei hohem Risiko: Durchführung einer DSFA, ggf. Konsultation der Aufsichtsbehörde
- Ergreifen von geeigneten Schutzmaßnahmen (TOMs)
- Dokumentation des ermittelten Risikos sowie der Implementierung von Schutzmaßnahmen
- Regelmäßige Re-Evaluation des Risikos

[489] Siehe hierzu Abschnitt: 7.1.1.
[490] *Gausling*, DSRITB 2018, 519 (535).

5.5 Richtigkeit

Mit dem Grundsatz der Richtigkeit wird dem Verantwortlichen die Pflicht auferlegt, die Richtigkeit der verarbeiteten personenbezogenen Daten aus eigener Initiative aktiv zu überprüfen.[491] Nach ErwGr. 39 S. 11 DSGVO sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

> **Art. 5 Abs. 1 Buchst. d DSGVO** Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden

Aus dem Grundsatz der Richtigkeit der Daten ergibt sich somit bereits eine Löschpflicht auf Seiten des Verantwortlichen.[492] Auch der Anspruch auf Berichtigung ist hier verankert. „Sachlich richtig" ist ein objektives Kriterium bei Tatsachenangaben und dann erfüllt, wenn die über die betroffene Person gespeicherten Informationen mit der Realität übereinstimmen.[493] Bei Werturteilen kann hingegen weder von „richtig" noch „unrichtig" gesprochen werden, da diese subjektiver Natur sind.[494] Da der Output von KI-Systemen oftmals nur eine Prognose ist, stellt sich die Frage, ob der Grundsatz der Richtigkeit nur auf den Dateninput bezogen werden sollte.[495]

Mit dem Zusatz „erforderlichenfalls" wird deutlich, dass die Daten nicht in jedem Fall auf dem neuesten Stand sein müssen – oftmals dürften sich Angaben auch auf bestimmte Zeitpunkte beziehen.[496] Kommt es auf den jeweiligen historischen Kontext an, machen nachträgliche Veränderungen der Wirklichkeit, wie bspw. die Änderung von Vor-/Nachnamen oder der Geschlechtszugehörigkeit, die gespeicherten personenbezogenen Daten nicht falsch – insbesondere wenn es um die Dokumentation eines historischen Geschehensablaufs geht.[497] Insofern besteht hier auch ein enger Bezug zum Verarbeitungszweck (vgl. Abschnitt 5.3).

Im Rahmen des Profilings weist ErwGr. 71 DSGVO darauf hin, dass der Verantwortliche technische und organisatorische Maßnahmen treffen muss, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird. Bei der Auswahl von geeigneten Trainingsdaten für KI-Systeme stellt sich insofern auch die Frage, wie mit historisch „richtigen", allerdings im Nachhinein als diskriminierend einzustufenden Daten umzugehen ist: hier besteht die Gefahr, dass sich Fehlentscheidungen der Vergangenheit in der Zukunft verfestigen.

---

[491] *Pötters,* in: Gola DS-GVO, Art. 5 Rn. 24; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 5 Rn. 24; *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 28.

[492] vgl. *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 41. Zu den Löschpflichten siehe Abschnitt 2.4.6.1.

[493] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 60; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 139.

[494] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 60; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 140; a.A. *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 27. Auch Werturteile insbesondere Prognosen und Korrelationen könnten falsch sein, wenn sie auf fehlerhafter Tatsachengrundlage beruhen, von falschen Prämissen ausgehen oder das Ergebnis unrichtiger Schlussfolgerungen sind.

[495] *Gausling*, DSRITB 2018, 519 (535).

[496] OVG Hamburg, Urteil vom 27.5.2019, Az. 5 Bf 225/18.Z, Rn. 22; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 61; vgl. auch *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 40; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 5 Rn. 24; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 141.

[497] OVG Hamburg, Urteil vom 27.5.2019, Az. 5 Bf 225/18.Z, Rn. 22.

5.5.1 Recht auf Berichtigung

Art. 16 S. 1 DSGVO gewährt der betroffenen Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Der Anspruch ergänzt den Grundsatz der Datenrichtigkeit.[498]

Ausübung des Rechts: Ein Berichtigungsantrag kann formlos (schriftlich, mündlich, elektronisch, etc.) gestellt werden und ist kostenfrei.[499] Es muss lediglich substantiiert dargelegt werden, dass die personenbezogenen Daten der betroffenen Person unrichtig sind.[500]

Unverzügliche Berichtigung: Nach dem üblichen juristischen Sprachgebrauch meint „unverzüglich" regelmäßig „ohne schuldhaftes Zögern" (vgl. § 121 Abs. 1 S. 1 BGB).[501] Ergänzend setzt Art. 12 Abs. 3 S. 1 eine absolute Frist von einem Monat für die Entscheidung über den Berichtigungsantrag. Diese Frist kann gemäß Art. 12 Abs. 3 S. 2 DSGVO um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Verzögert sich die Berichtigung kann die betroffene Person gemäß Art. 18 Abs. 1 Buchst. a DSGVO die Einschränkung der Verarbeitung verlangen (ob ein Antrag auf Berichtigung gleichzeitig eine Einschränkung der Verarbeitung impliziert, ist im Wege der Auslegung zu ermitteln).[502]

Berichtigung: Die Korrektur der Daten kann durch eine Veränderung, vollständige oder teilweise Löschung, Vervollständigung oder ergänzende Klarstellung erfolgen.[503] Der Verantwortliche ist ferner nach Art. 19 S. 1 DSGVO verpflichtet, etwaige Empfänger, denen die berichtigten Daten offengelegt wurden, über die Berichtigung zu informieren. Diese Informationspflicht entfällt, wenn sie sich als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist. Verlangt die betroffene Person eine Unterrichtung über die Empfänger, trifft den Verantwortlichen nach Art. 19 S. 2 DSGVO die Pflicht diese umzusetzen.

Unrichtige Daten: Unstreitig sind Tatsachen, die einem empirischen Beweis zugänglich sind und nicht mit der Realität übereinstimmen (bzw. zum maßgeblichen Zeitpunkt nicht übereinstimmten), als unrichtig zu berichtigen – unabhängig davon auf welcher Ursache die Unrichtigkeit beruht.[504] Problematischer ist die Frage bei Werturteilen.[505] Einige wollen diese von vorneherein herausnehmen, da sie weder „richtig" noch „falsch" sein können, sondern eine Meinung repräsentieren.[506] Andere präferieren ein differenziertes Vorgehen: Werturteile von Privaten fallen unter die Meinungsfreiheit und unterfallen – sofern keine Tatsachenbestandteile enthalten sind – nicht dem Anwendungsbereich der Berichtigungspflicht. Ein solcher Schutz gelte hingegen nicht für öffentliche Stellen.[507] Andere wiederum präferieren stets eine Grundrechtsabwägung, insbesondere vor dem Hintergrund, dass sich Werturteil und Tatsachengrundlagen oftmals nicht klar trennen lassen. [508] Insofern lässt sich aktuell nicht abschließend sagen, welche personenbezogene Daten vom Berichtigungsanspruch erfasst werden.

---

[498] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 2.
[499] *Reif,* in: Gola DS-GVO, Art. 16 Rn. 17.
[500] *Kammann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 22; *Reif,* in: Gola DS-GVO, Art. 16 Rn. 17.
[501] *Reif,* in: Gola DS-GVO, Art. 16 Rn. 18; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 23.
[502] *Reif,* in: Gola DS-GVO, Art. 16 Rn. 18.
[503] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 18 ff.
[504] *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 52; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 8 ff.
[505] Siehe zur Behandlung von Werturteilen in der Rechtsprechung: *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 19 m.w.N.
[506] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 8; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 140; *Reif,* in: Gola DS-GVO, Art. 16 Rn. 10.
[507] *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 55.
[508] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 21.

5.5.2 Recht auf Vollständigkeit

Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person nach Art. 16 S. 2 DSGVO das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. Dies lässt sich als Spezialfall der in Satz 1 genannten Berichtigung sehen.[509] Wann Daten unvollständig sind, lässt sich nur *relativ* anhand des konkret verfolgten Verarbeitungszecks feststellen.[510] Eine der Unrichtigkeit gleichstehende Bedeutung besteht, wenn die Daten zwar für sich genommen richtig sind, aber in der Gesamtheit eine objektiv falsche Aussage treffen oder durch die Lückenhaftigkeit objektiv missverständlich sind. [511] Folglich kommt es auf den Gesamtkontext an.[512] Eine Berichtigungspflicht soll zudem nur bestehen, wenn die Vervollständigung im Hinblick auf die Zwecke relevant ist. [513] Als Unterfall des Berichtigungsanspruchs soll die Vervollständigung ebenfalls „unverzüglich" erfolgen und die Mitteilungspflichten nach Art. 19 DSGVO auslösen.[514]

5.5.3 Zwischenergebnis zum Grundsatz der Richtigkeit

Den Verantwortlichen treffen die folgenden Pflichten und Organisationsobliegenheiten:

- Angemessene Maßnahmen zur regelmäßigen Prüfung auf Unrichtigkeit und aktive Berichtigung bzw. Löschung unrichtiger Daten sowie ggf. Aktualisierung veralteter Daten.
- Etablierung organisatorischer Maßnahmen zur Umsetzung bzw. Beantwortung von Berichtigungsanfragen innerhalb der gesetzlichen Fristen sowie ggf. Mitteilung an etwaige Empfänger der Daten über die Berichtigung.
- Vorsehen von Möglichkeiten einer Einschränkung der Verarbeitung für die Dauer, die der Verantwortliche benötigt, um die Richtigkeit der personenbezogenen Daten zu überprüfen.

5.6 Speicherbegrenzung

Dieser Grundsatz legt eine zeitliche Begrenzung für die Verarbeitung personenbezogener Daten fest. Da das Training künstlicher Neuronaler Netze regelmäßig eine große Menge an Daten erfordert, steht dieses Prinzip zwangsläufig im Konflikt mit der Entwicklung von KI-Systemen.[515] Laut Art. 5 Abs. 1 Buchst. e DSGVO dürfen die gespeicherten Daten die betreffende Person nur so lange identifizieren oder zu ihrer Identifizierung beitragen, wie es für den Zweck der Verarbeitung erforderlich ist. Löschpflichten sind in Art. 17 DSGVO normiert. Konkretisierend schlägt ErwGr. 39 S. 9 und S.10 die Verwendung von Löschfristen vor.

> **Art. 5 Abs. 1 Buchst. e DSGVO** Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

[509] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 4.
[510] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 26; *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 36; *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 58; *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 16 Rn. 18.
[511] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 36; *Meents/Hinzpeter,* in: Taeger/Gabel - DSGVO/BDSG Art. 16 Rn. 21.
[512] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 36.
[513] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 37; *Dix,* in: NK Datenschutzrecht Art. 16 Rn. 18; *Meents/Hinzpeter,* in: Taeger/Gabel - DSGVO/BDSG Art. 16 Rn. 21.
[514] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 30, 31; *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 16 Rn. 20; *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 62; *Dix,* in: NK Datenschutzrecht Art. 16 Rn. 18.
[515] *Gausling*, DSRITB 2018, 519 (533 f.).

[...]

5.6.1 Löschpflichten

Mit dem Recht auf Löschung gewährt die DSGVO der betroffenen Person einen Anspruch, vom Verantwortlichen die unverzügliche Löschung ihrer personenbezogenen Daten zu fordern, sofern einer der nachfolgenden in Art. 17 Abs. 1 DSGVO dargelegten Fälle vorliegt.

5.6.1.1 Löschgründe

Zweck der Verarbeitung entfallen (Buchst. a) Wenn und soweit die personenbezogenen Daten der betroffenen Person für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, hat eine Löschung zu erfolgen. Die Pflicht zur Löschung entfällt jedoch, soweit eine zulässige Zweckänderung (vgl. Art. 6 Abs. 4 DSGVO) vorliegt und die Daten für diesen neuen Zweck noch erforderlich sind.[516]

Widerruf der Einwilligung (Buchst. b) Ist die Datenverarbeitung auf eine Einwilligung gemäß Art. 6 Abs. 1 Buchst. a oder Art. 9 Abs. 2 Buchst. a DSGVO gestützt, so hat bei Widerruf dieser Einwilligung eine Löschung zu erfolgen, sofern eine weitere Rechtsgrundlage für die Verarbeitung nicht vorhanden ist. Umstritten ist, ob hiermit trotz Widerruf der Einwilligung ein Wechsel der Rechtsgrundlage möglich ist.[517] Dies würde der betroffenen Person allerdings nur eine Autonomie suggerieren, wenn die Ausübung ihres Widerrufsrechts praktisch „ins Leere laufen“ würde.[518] Mit dem Verweis auf die fortdauernde Rechtfertigung auf Basis anderweitiger Rechtsgrundlagen zeigt diese Norm richtigerweise vielmehr auf, dass die ursprüngliche Verarbeitung gleichzeitig auf mehrere Erlaubnistatbestände, also eine Einwilligung und gleichzeitig eine andere Rechtsgrundlagen gestützt werden kann.[519] Ist die Datenverarbeitung zur Zweckerreichung dieser weiteren Rechtsgrundlage weiterhin erforderlich, muss keine Löschung erfolgen.[520] Ein Teilwiderruf (d.h. entweder auf Teile der Einwilligung oder Teile der Verarbeitung) soll hingegen keinen wirksamen Löschungsgrund für die nicht erfassten Teile begründen. Konsequenterweise soll bei Untrennbarkeit dieser Teile auch kein Löschungsgrund i.S.v. Buchst. b vorliegen.[521]

Widerspruch (Buchst. c) Legt die betroffene Person Widerspruch gemäß Art. 21 Abs. 1 DSGVO gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, so hat eine Löschung zu erfolgen. Liegt ein Widerspruch nach Art. 21 Abs. 2 DSGVO (Widerspruchsrecht im Rahmen von Direktwerbung) vor, hat eine Löschung ohne weitere Bedingung zu erfolgen.

Unrechtmäßige Verarbeitung (Buchst. d) Wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden, hat eine Löschung zu erfolgen. Entgegen der missverständlichen Formulierung (”verarbeitet wurden”), soll die *gegenwärtige* Recht- bzw. Unrechtmäßigkeit der Verarbeitung maßgeblich sein.[522] Die Unrechtmäßigkeit soll nicht nur vorliegen, wenn ein Rechtmäßigkeitsgrund i.S.v. Art. 6 bzw. Art. 9 DSGVO fehlt,

[516] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 23.
[517] *Plath,* in: *Plath*, Plath, DSGVO/BDSG Art. 7 Rn. 15.; *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 91.1.
[518] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 23.
[519] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 23 ff.
[520] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 24.
[521] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 25.
[522] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 26.

sondern nach ErwGr. 65 auch, wenn die Verarbeitung "aus anderen Gründen" gegen die DSGVO verstößt.[523]

Erfüllung einer rechtlichen Verpflichtung (Buchst. e) Eine Löschung hat ebenfalls zu erfolgen, wenn und soweit die Löschung zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten, dem der Verantwortliche unterliegt, erforderlich ist. Ob Mitgliedsstaaten aufgrund dieser Regelung ermächtigt sind, Löschpflichten zu erlassen, ist jedoch umstritten.[524] Der Begriff der rechtlichen Verpflichtung soll dabei aber weit verstanden werden und sich nach Art. 6 Abs. 1 Buchst. c DSGVO richten: Demnach muss es ich um eine Rechtspflicht nach objektivem und hinreichend klarem sowie vorhersehbaren Recht handeln und muss nicht zwingend die Form eines Gesetzes haben. Rechtskräftige Entscheidungen von Behörden und Gerichten sollen daher ebenfalls ausreichend sein.[525]

5.6.1.2 Unverzüglichkeit

Beim Vorliegen einer der vorgenannten Fälle, sind die Daten mit Personenbezug unverzüglich zu löschen. „Unverzüglich" bedeutet in diesem Zusammenhang, dass einzelfallabhängig anhand der konkreten Verarbeitung und dem damit verbundenen Löschungsaufwand bestimmt werden muss, wann eine Löschung zu erfolgen hat.[526] Bei der Prüfung der Zeitspanne ist v.a. zu berücksichtigen, dass dem Verantwortlichen ausreichend Zeit für die rechtliche Prüfung der Ausschlusstatbestände in Art. 17 Abs. 3 DSGVO eingeräumt werden muss.[527] Fraglich ist, ob sich daher eine pauschale Gleichsetzung mit dem Begriff der Unverzüglichkeit aus Art. 16 S. 1 DSGVO verbietet.[528] Anhaltspunkte können hier zwar Art. 12 Abs. 3, 4 DSGVO liefern, der ein Tätigwerden ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags fordert.[529] Zu beachten ist jedoch, dass die Frist von einem Monat bereits die Ausnahme und damit die zeitliche Obergrenze darstellt.[530] Im Einzelfall soll folglich eher ein kürzerer aber ausnahmsweise auch längerer Zeitraum in Betracht kommen.[531]

5.6.1.3 Umsetzung der Löschung

Eine Definition von Löschen existiert in der DSGVO nicht, es wird auch keine spezifische Löschmethode vorgeschrieben.[532] Durch die alternative Erwähnung des Begriffs des Löschens neben dem Begriff der Vernichtung in Art. 4 Nr. 2 DSGVO lässt sich aber ableiten, dass beide Begriffe nicht synonym zu gebrauchen sind und ein Unterschied besteht. [533] Das BDSG a.F. definierte das Löschen in § 3 Abs. 4 Nr. 5 als „Unkenntlichmachen gespeicherter personenbezogener Daten". „Vernichten" bezeichnet die physische Zerstörung des Datenträgers. Da Datenträger allerdings regelmäßig nur überschrieben werden, meint Löschung im technischen Sinn

[523] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 27.
[524] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 27; *Worms,* in: BeckOK DatenschutzR Art. 17 Rn. 45; *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 16; *Nolte/Werkmeister,* in: Gola DS-GVO, Art. 17 Rn. 26.
[525] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 28; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 30; *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 16.
[526] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31.
[527] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31; *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 8; *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 38.
[528] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31.
[529] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 46; *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31; *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 38.
[530] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 40.
[531] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31; *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 40; a.A. *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 8 (wonach die Monatsfrist nicht überschritten werden dürfe).
[532] *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 5; *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 31.
[533] *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 32.

einen Vorgang, nach dessen Ende auf die Daten bzw. deren Inhalt nicht mehr mit den üblichen Verfahren zugegriffen werden kann – es also unmöglich ist, die in den Daten verkörperte Information wahrzunehmen.[534] Entscheidend ist, dass die Daten nicht mehr verarbeitet und zu diesem Zweck auch nicht mehr ohne übermäßigen Aufwand wiederhergestellt werden können.[535] Daten können demnach

- durch ordnungsgemäße Vernichtung des betreffenden Datenträgers oder
- durch (mehrfaches) Überschreiben gelöscht werden (physikalische Löschung).

Die bloße Löschung einer Verknüpfung, eines Verweises im Dateisystem oder einer Zugriffsmöglichkeit auf einen Datensatz (auch logische Löschung genannt) führt dagegen regelmäßig nicht zu einer tatsächlichen Löschung, sondern macht den Datensatz höchstens schwerer auffindbar.[536] Im Hinblick auf die technische Umsetzung gilt zu beachten, dass der Erfolg der Löschungshandlung bei auf einem wiederbeschreibbaren Datenträger zu löschenden Daten, nicht schon dann eintritt, wenn die betreffenden Speicherplätze zum neuen Beschreiben freigegeben sind, sondern erst beim tatsächlichen Überschreiben.[537] Dies bedeutet, dass die in den Betriebssystemen zur Verfügung stehenden einfachen Löschbefehle nicht ausreichen: In diesen Fällen kann der Einsatz von Löschsoftware notwendig werden.[538]

Praxistipp

Im IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) befasst sich ein Baustein mit Löschen und Vernichten und gibt einen Überblick über Methoden zur Löschung und Vernichtung von Daten.[539] Im Bereich der technischen Normungen kann zudem – je nach Fallgestaltung – auf die DIN 66398 (Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten) sowie die DIN 66399 (Büro- und Datentechnik - Vernichtung von Datenträgern) zurückgegriffen werden.[540] Im Rahmen des Standard-Datenschutzmodells bietet Baustein 60 „Löschen und Vernichten“ Hinweise zur Umsetzung der DSGVO.[541]

Im Hinblick auf KI-Anwendungen, die auf großen Datenmengen basieren („Big Data“) wird diskutiert, ob eine Separierung der Daten, welche einem Löschbegehren unterliegen, technisch möglich ist, ohne den Gesamterfolg des Systems zu gefährden.[542] Insofern wird von Stimmen aus der Literatur erwogen, ob die Betroffenenrechte mit Blick auf eine Abwägung der Grundrechtspositionen der unternehmerischen Freiheit (Art. 16, 17 EU-GrCh) einerseits und der Datenschutzgrundrechte (Art. 7, 8 EU-GrCh) andererseits insgesamt eingeschränkt werden könnten.[543] Bisher ist dies nur für privilegierte Zwecke unter der Voraussetzung angemessener (kompensierender) Schutzgarantien nach Art. 89 DSGVO vorgesehen (siehe zu Forschung: Abschnitt 9.3). *Kammann/Braun* argumentieren, aus Verhältnismäßigkeitserwägungen sei auch hier die Möglichkeit eines

[534] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 29; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 37.
[535] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 30.
[536] *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 5; a.A. wohl *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 39.
[537] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 38.
[538] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 38.
[539] BSI, IT-Grundschutz-Kompendium, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6 [letzter Abruf 18.08.2021].
[540] Siehe hierzu https://www.din.de/de/wdc-beuth:din21:249218525 [letzter Abruf 18.08.2021].
[541] SDM - Baustein 60 “Löschen und Vernichten”, Version V1.0a, abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell [letzter Abruf 18.08.2021].
[542] *Niemann/Kevekordes*, CR 2020, 179 (182).
[543] *Niemann/Kevekordes*, CR 2020, 179 (182).

Unzumutbarkeitseinwands angemessen.[544] Andere wollen die Löschpflicht auf „ad hoc verfügbare personenbezogenen Daten“ beschränken. [545] Weitere Vorschläge betreffen die analoge Anwendung von Art. 14 Abs. 5 DSGVO. [546] Andererseits zählt die technische Gestaltung der Prozesse auf eine Art und Weise, das Löschrechte effektiv verwirklicht werden können, zu den Privacy-by-Design-Prinzipien nach Art. 25 Abs. 1 DSGVO. Dies gilt auch für Big Data.[547] Wurden Daten derart aggregiert oder anonymisiert, dass eine Identifizierung und damit Zuordnung der Daten zu einer Einzelperson nicht mehr möglich ist, greift Art. 11 Abs. 2 DSGVO (siehe Abschnitt 5.2.3.3 im Rahmen der Auskunftsrechte). Daher ist nicht davon auszugehen, dass es an der für eine Analogie erforderlichen planwidrigen Regelungslücke fehlt.

5.6.1.4 Ausnahmen von der Löschpflicht

Art. 17 Abs. 1 und 2 DSGVO gelten jedoch nicht, soweit die Verarbeitung erforderlich und einer der nachfolgenden und in Art. 17 Abs. 3 DSGVO dargelegten Fälle vorliegt. Ein Recht zur Löschung soll demnach in folgenden Fällen nicht bestehen:

Freie Meinungsäußerung (Buchst. a) Eine Löschung hat nicht zu erfolgen, soweit die Verarbeitung zur Ausübung des Rechtes auf freie Meinungsäußerung und Information (Art. 11 Abs. 1 GrCh) erforderlich ist.

Rechtliche Verpflichtung (Buchst. b) Der Verantwortliche hat dem Löschgesuch nicht zu entsprechen, soweit die Verarbeitung für die Erfüllung bestimmter rechtlicher Verpflichtungen bzw. für bestimmte Aufgabenwahrnehmungen erforderlich ist. Zu den rechtlichen Verpflichtungen wird auf die Ausführungen zu Art. 6 DSGVO unter 6.5 verwiesen.

Öffentliches Interesse (Buchst. c) Ein Löschrecht ist ebenfalls nicht gegeben, soweit die Verarbeitung erforderlich ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Abs. 2 Buchst. h und i sowie Artikel 9 Abs. 3 DSGVO.

Archiv, Forschung und Statistik (Buchst. d) Eine gewisse Aufweichung des Grundsatzes der Speicherbegrenzung besteht bei im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder für statistische Zwecke gemäß Artikel 89 Abs.1 DSGVO, soweit das Löschrecht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.[548]

Rechtsansprüche (Buchst. e) Wenn der Zweck der Verarbeitung wegfällt, die betroffene Person die Daten aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Aus der Formulierung „benötigt” ergibt sich, dass zumindest eine hinreichende Wahrscheinlichkeit für eine rechtliche Auseinandersetzung bestehen muss.[549]

Mangelnde Identifizierbarkeit: Eine weitere Ausnahme besteht im Rahmen des Art. 11 DSGVO. Dieser trägt dem Umstand Rechnung, dass bei mangelnder Möglichkeit Daten einer konkreten Person zuzuordnen, eine Pflicht zur Verknüpfung mit weiteren, identifizierenden Daten, regelmäßig nicht der Zielsetzung des Da-

[544] *Kammann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 39.
[545] *Nolte/Werkmeister,*in: Gola DS-GVO, At. 17 Rn. 34.
[546] *Niemann/Kevekordes*, CR 2020, 179 (182) m.w.N.
[547] *Nolte/Werkmeister,*in: Gola DS-GVO, At. 17 Rn. 34.
[548] Zu Privilegien der Forschung siehe: *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, S. 23; *Johannes/Richter,* DuD 2017, 300 (301); *Molnár-Gábor,* DSRITB 2018, 159 (164); *Wirth,* ZUM 2020, 585 (591 ff.).
[549] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 18 Rn. 22 f.

tenschutzes entspricht. Gleichwohl gibt er der betroffenen Person die Möglichkeit durch Bereitstellung weiterer Daten ihre Rechte wahrzunehmen.

5.6.2 „Recht auf Vergessenwerden"

Das Recht auf Vergessenwerden hatte bereits der EuGH mit dem Urteil *Google v. Spain* im Jahr 2014 auf Grundlage des Rechts auf Löschung aus der Datenschutz-Richtlinie abgeleitet.[550] Mit der DSGVO wurde in Art. 17 Abs. 2 DSGVO nun Klarheit darüber geschaffen, dass betroffene Personen gegenüber dem für die Verarbeitung Verantwortlichen verlangen können, nach einer Veröffentlichung ihrer personenbezogenen Daten ein Löschungsverlangen an andere Stellen weiterzuleiten.[551]

> **Art. 17 Abs. 2 DSGVO** Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

5.6.3 Zwischenergebnis zum Grundsatz der Speicherbegrenzung

Da sich die Löschpflichten nach der Zweckerreichung und damit der verfolgten Zielsetzung und zu Grunde liegenden Rechtsgrundlage richten, kann es je nach Datenverarbeitungsvorgang zu unterschiedlichen Löschfristen kommen. Daher ist ein Löschmanagement essentiell, um vorab ggf. für unterschiedliche Datenkategorien unterschiedliche Löschfristen vorzusehen. Im Rahmen der Transparenzpflichten muss die Speicherdauer oder zumindest die Kriterien für die Festlegung dieser Speicherdauer den betroffenen Personen mitgeteilt werden. Vorbedingung hierfür ist es, dass sich der:die Verantwortliche*n zunächst selbst einen Überblick über die betroffenen Daten, die Verarbeitungsschritte, die Verarbeitungszwecke und die dafür jeweils einschlägigen Rechtsgrundlagen macht.

5.7 Datensicherheit

Art. 5 Abs. 1 Buchst. f DSGVO enthält den Grundsatz der „Integrität und Vertraulichkeit". Dieses Datenschutzprinzip wird in Art. 32 DSGVO konkretisiert und erlegt dem Verantwortlichen sowie dem Auftragsverarbeiter (teilweise gemeinsam) die Pflicht zur Sicherung der Daten auf.

> **Art. 5 Abs. 1 Buchst. f DSGVO** Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger

[550] EuGH, Urteil vom 13.05.2014 – C-131/12 – Google/Spain.
[551] *Albrecht*, CR 2016, 88 (93).

Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen

5.7.1.1 Bedeutung des risikobasierten Ansatzes

Im Hinblick auf ein angemessenes Schutzniveau gelten die bereits durch den risikobasierten Ansatz[552] nach Art. 25 Abs. 1 DSGVO bekannten Kriterien:

- Stand der Technik,
- Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung sowie
- unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Art. 32 Abs. 2 DSGVO weist zudem darauf hin, dass bei der Beurteilung des angemessenen Schutzniveaus die Risiken zu berücksichtigen sind, die mit der Datenverarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugter Zugang und unbefugte Offenlegung von personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

5.7.1.2 Umsetzungsmöglichkeiten

Art. 32 Abs. 1 DSGVO bietet neben den Abwägungskriterien zur Bestimmung risikoadäquater „geeigneter technischer und organisatorischer Maßnahmen“ (TOMs) zur Erreichung eines angemessenen Schutzniveaus auch Beispiele solcher Maßnahmen. Mit den Worten „gegebenenfalls unter anderem“ wird deutlich, dass es sich nur um eine Aufzählung nicht abschließender Beispiele handelt:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Hierbei gilt zu bedenken, dass die Auswahl geeigneter TOMs, insbesondere unter Berücksichtigung des (jeweils aktuellen) Stands der Technik, nicht eine einmalige Maßnahme bleiben darf, sondern mittels einer transparenten Methode zum Vergleich der am Markt verfügbaren Alternativen regelmäßig wiederholt werden sollte.[553]

Pseudonymisierung: Soweit einer Pseudonymisierung unterzogene Daten durch Heranziehung zusätzli-

[552] Dieser gilt auch im Rahmen des Art. 32 DSGVO: *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 9.
[553] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 12.

cher Informationen einer natürlichen Person zugeordnet werden können, werden diese weiterhin als personenbezogene Daten zu betrachten sein (vgl. ErwGr. 26 S. 2 DSGVO).[554] Entsprechend der Definition der Pseudonymisierung kann diese nicht bei jeglichem Ersetzen des bürgerlichen Namens durch eine Kennziffer vorliegen, wenn diese Daten ohne Weiteres einer identifizierbaren Person zugeordnet werden können.[555] Zwar werden als Beispiele für Pseudonyme auch Künstlernamen, Telefonnummern, E-Mail-Adressen, Benutzernamen und Personalnummern genannt.[556] Sog. „offene Pseudonyme“[557] wie Telefonnummern, deren Zuordnung zu einer konkreten Person über öffentlich zugängliche Telefonverzeichnisse oder ähnliches leicht umsetzbar ist, und „Personenpseudonyme“,[558] die einer Person fest zugewiesen sind, erfüllen allerdings kaum die Anforderungen der Definition. Zu unterscheiden ist somit zwischen dem Pseudonym nach allgemeinem Sprachgebrauch, das bereits bei der Ersetzung des Namens durch einen erfundenen „Decknamen“ oder eine Kennziffer gegeben ist, und der Pseudonymisierung i.S.d. Art. 4 Nr. 5 DS-GVO.[559] Insofern wird vorgeschlagen, zwischen formaler, faktischer und absoluter Pseudonymität zu differenzieren.[560] Entsprechend erhöht oder senkt die Pseudonymisierung das Schutzlevel.

Verschlüsselung: Je nach Kontext haben sich unterschiedliche Verschlüsselungsverfahren etabliert. Im Hinblick auf Datenübermittlungen hob die DSK hervor, dass sowohl Ende-zu-Ende-Verschlüsselung als auch Transportverschlüsselung von Verantwortlichen mindestens im Rahmen der Abwägung notwendiger Maßnahmen berücksichtigt werden müssen.[561]

CIA-Schutzziele: In der IT-Sicherheit werden klassischerweise die Schutzziele Vertraulichkeit (**C**onfidentiality), Integrität (**I**ntegrity) und Verfügbarkeit (**A**vailability) fokussiert sowie um die Ziele Authentizität, Verbindlichkeit, Resilienz, und Anonymität erweitert.[562] „Cybersicherheit“ bezeichnet „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.“[563] Grundsätzlich empfiehlt die DSK zur Gewährleistung der Vertraulichkeit die Verwendung lokaler KI-Komponenten mit direkt anschließender Löschung der Daten.[564] Zur Sicherstellung der Integrität können klassische Methoden der IT-Sicherheit zum Schutz vor Manipulation genutzt werden, wie z. B. die digitale Signatur von Trainingsdaten oder von Systemparametern, sowie Festlegung eines Rechte- und Rollenkonzepts, welche:r Systembetreuer*in welche Rechte am System hat.[565]

Schutzziele		Beschreibung	Typische Angriffe
Confidentiality	Vertraulichkeit	Schutz vor dem Abhören / Mitlesen von Daten; Zugriff auf Informationen und Systeme nur durch Berechtigte möglich	Man-in-the-Middle
Integrity	Integrität	Schutz vor der Manipulation von Daten; Informati-	

[554] Siehe hierzu: *Roßnagel/Scholz*, MMR 2000, 721 (725).
[555] *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 42.
[556] *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 94.
[557] Zum Begriff siehe: *Roßnagel/Scholz*, MMR 2000, 721 (727); ähnlich *Probst*, in: Bäumler/von Mutius, Anonymität im Internet, S. 179 (185).
[558] Zum Begriff siehe: *Hansen*, in: Bäumler/von Mutius, Anonymität im Internet, S. 198 (205).
[559] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 506 ff.
[560] *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 98.
[561] *DSK - Datenschutzkonferenz*, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, S. 3.
[562] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 14; *Rockstroh/Kunkel*, MMR 2017, 77 (78); *Heckmann*, MMR 2006, 280 (281); *Bräutigam/Klindt*, NJW 2015, 1137 (1141). Vgl. auch § 2 Abs. 2 BSIG.
[563] Art. 2 Nr. 1 Cybersecurity Act.
[564] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 15.
[565] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 15.

		onen sind inhaltlich korrekt, unversehrt und vollständig	
Availability	Verfügbarkeit	Schutz vor Systemausfällen; Informationen sind für Berechtigte zugänglich und nutzbar	Denial-of-Service
Authenticity	Authentizität	Garantie für Echtheit einer Nachricht / Vertrauenswürdigkeit von Daten	Spoofing
Non-Repudiation	Verbindlichkeit	Eine Partei kann eine durchgeführte Handlung nicht abstreiten; eindeutige Zuordnung zu einer Quelle	
Resilience	Resilienz	Widerstandsfähigkeit gegenüber Sabotage	
Anonymity	Anonymität	Schutz der Identität	De-Anonymisierung

Tabelle 3 Schutzziele der Informationssicherheit

In Anlehnung an das Standard-Datenschutzmodell[566] können diese Ziele noch um die Ziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit ergänzt werden.[567] Zur Sicherung der Vertraulichkeit sollten im Unternehmenskontext vorab feste Kommunikationswege festgelegt werden, welche auch in Krisenzeiten beibehalten werden können.[568]

Überprüfung: Empfohlen wird, die Umsetzung der Sicherheitsfunktionen durch vertrauenswürdige Dritte überprüfen zu lassen.[569] In diesem Sinne fallen auch sog. Penetrationstests (kurz: Pentests) unter Art. 32 Abs. 1 Buchst. d DSGVO.[570] Werden Systeme von Fremdherstellern eingesetzt, sollte geprüft werden, ob diese solche Pentests und ähnliche Sicherheitsüberprüfungen ausschließen oder explizit erlauben. Denn sowohl aus Urheber- als auch Strafrechtlicher Sicht kann es u.U. zu Implikationen kommen, wenn Nutzer*innen ohne Einverständnis der jeweiligen Rechteinhaber Softwaretests durchführen (bzw. von Dritten durchführen lassen), welche unterschiedliche Formen des Reverse-Engineerings beinhalten.[571] Handelt es sich um Open-Source-Code, ist damit in der Regel die Befugnis zur Bearbeitung und damit auch Formen der Sicherheitsüberprüfungen wie Disassemblieren oder Dekompilieren des Codes erlaubt.[572] Bei der Auswahl eines geeigneten Angebots kann auch darauf geachtet werden, ob der Anbieter über eine Responsible-Disclosure-Policy verfügt. Diese Policy regelt wie durch Dritte gefundene Sicherheitslücken an den Hersteller gemeldet werden können.[573]

Assume-Breach-Paradigma: Da immer wieder neue, zuvor noch unbekannte Sicherheitslücken (sog. „Zero-Day-Schwachstellen“) entdeckt werden, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) stets davon auszugehen, dass ein Produkt Schwachstellen enthält.[574] Insofern ist hervorzuheben, dass

[566] Siehe Abschnitt 2.4.4.2.5.1.
[567] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 15.
[568] vgl. *Gilga*, ZD-Aktuell 2020, 07113.
[569] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 17.
[570] *Hladjk,* in: Ehmann/Selmayr - DSGVO Art. 32 Rn. 10; *Jandt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 32 Rn. 29; *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 32 Rn. 44; *Mantz,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 32 Rn. 20; *Hansen,* in: NK Datenschutzrecht Art. 32 Rn. 56.
[571] *Maier u. a.*, DuD 2020, 511; *Wagner*, PinG 2020, 66 (71); *Wagner*, DuD 2020, 111.
[572] Vgl. zur GPL: *Hoeren,* in: Westphalen/Thüsing - Vertragsrecht und AGB-Klauselwerke, Kap. IT-Vertäge Rn. 210.
[573] *European Network and Information Security Agency (ENISA)*, Good practice guide on vulnerability disclosure, S. 56 ff.; *Pupillo u. a.*, Software vulnerability disclosure in Europe, S. 80; *National Cyber Security Centre*, Coordinated Vulnerability Disclosure: the Guideline, S. 21 ff.
[574] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2017, S. 18; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, S. 22 ff.; BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 38.

Sicherheitskonzepte eine ganzheitliche Sicherheitsarchitektur für den gesamten Produktlebenszyklus, angepasst an die jeweiligen Konfigurationsmöglichkeiten bieten sollten.[575] Trifft den Hersteller des Kommunikationssystems keine direkte Verpflichtung zur Umsetzung der Anforderungen aus Art. 32 DSGVO (sofern dieser als Produktlieferant nicht selbst Verantwortlicher oder Auftragsverarbeiter ist), sollten Unternehmen entsprechende Update-Services (ggf. gesondert) vereinbaren. Denn als Unternehmer i.S.d. § 14 BGB profitieren sie nicht von der durch die Digitale-Inhalte-Richtlinie (Richtlinie (EU) 2019/770) sowie Warenkauf-Richtlinie (Richtlinie (EU) 2019/771) forcierten Novellierungen im BGB zu Update-Pflichten (§ 327f BGB, § 475b BGB) für Digitale Produkte und Waren mit digitalen Elementen, da diese nur Verbraucher*innen i.S.d. § 13 BGB schützen.[576]

Dokumentation: Der Stand der Technik sollte im Rahmen des IT-Sicherheitsmanagements nicht nur berücksichtigt, sondern auch dokumentiert werden.[577]

5.7.1.3 Zwischenergebnis zur Datensicherheit und Bedeutung für die KI-Systemnutzung im Unternehmenskontext

Gerade kleine und mittelständische Unternehmen zeigten in der Vergangenheit wiederholt Schwierigkeiten, IT-Sicherheitsbedürfnisse und tatsächlich umgesetzte Sicherheitsmaßnahmen in Einklang zu bringen.[578] Um zu ermitteln, ob ein Dienst bzw. eine Software ein hohes Sicherheitsniveau bietet, können insbesondere folgende Aspekte Hinweise geben:

(1) Möglichkeit Anonymisierung / Pseudonymisierung
(2) Veröffentlichung externer Audits
(3) Veröffentlichung einer Responsible Disclosure Policy
(4) Dokumentation der Sicherheitskomponenten
(5) Sicherheitszertifikate

5.8 Rechenschaftspflicht

Der datenschutzrechtlich Verantwortliche unterliegt weitreichenden Rechenschaftspflichten, die sich unmittelbar aus datenschutzrechtlichen Vorgaben herleiten lassen. Gemäß Art. 5 Abs. 2, Alt. 2 DSGVO muss der Verantwortliche die Einhaltung aller datenschutzrechtlicher Grundsätze aus Art. 5 DSGVO nachweisen können. Da die Datenschutzgrundsätze zum einen für sich selbst stehen als auch in verschiedenen anderen Vorschriften ihre Konkretisierung finden, erstreckt sich die Rechenschaftspflicht des Verantwortlichen im Prinzip auf alle Datenverarbeitungsvorgänge mit Personenbezug.[579]

5.8.1 Verantwortlichkeit

Dieser Abschnitt widmet sich der konkreten Anforderungen im Hinblick auf die bereits eingeführten Konstellationen der gemeinsamen Verantwortung (Abschnitt 2.1.2.2) und der Auftragsverarbeitung (Abschnitt 2.1.3). Sind Anbieter*in und Nutzer*in des KI-Systems personenverschieden (und nicht gleichzeitig die betroffene

[575] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 17.
[576] Siehe zur Gesetzesnovelle: BT-Drs. 19/27653; BT-Drs. 19/27424.
[577] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 9.
[578] *Ziegler*, DuD 2021, 330 (330) m.w.N.
[579] Vgl. zur Bedeutung der Rechenschaftspflicht: *Jung*, ZD 2018, 208 (208 ff.).

Person selbst, sind folgende Konstellationen denkbar:

Alleinige Verantwortung	Auftragsverarbeitung	Gemeinsame Verantwortung
System-Anbieter:in liefert nur Software, verarbeitet keine personenbezogener Daten	System-Anbieter:in verarbeitet Daten nur im Auftrag des System-Nutzenden im Rahmen des Auftragsverarbeitungsvertrags	Anbieter:in und Nutzer*in tragen gemeinsam Verantwortung

Um abzugrenzen, ob eine Auftragsverarbeitung oder gemeinsame Verantwortung vorliegt, muss der:die das System in eigener Verantwortung Einsetzende die vorgelegten Vertragsvorlagen, Nutzungsbedingungen und Sicherheitsnachweise sowie die Datenschutzerklärung prüfen.[580] Selbst wenn der Vertrag als Auftragsverarbeitungsvertrag (AVV) bezeichnet ist, kann es sich um eine gemeinsame Verantwortlichkeit handeln, wenn der:die vermeintliche Auftragnehmer*in eigene Verarbeitungszwecke verfolgt.

5.8.1.1 Herausforderungen der gemeinsamen Verantwortlichkeit, Art. 26 DSGVO

Bei der gemeinsamen Verantwortlichkeit müssen die zwei oder mehreren Verantwortlichen nach Art. 26 Abs. 1 S. 2 DSGVO in einer Vereinbarung in transparenter Form festlegen,

- wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen angeht, und
- wer welchen Informationspflichten nachkommt,

sofern und soweit die jeweiligen Aufgaben nicht bereits durch andere Vorschriften festgelegt sind. Diese Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln (Art. 26 Abs. 2 S. 1 DSGVO). Diese klare Zuteilung hat auch Folgen für die Haftung sowie Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden (vgl. ErwGr. 79). Die Vereinbarung hat keinen Einfluss darauf, ob eine gemeinsame Verantwortlichkeit anzunehmen ist: sie ist weder Voraussetzung noch kann sie eine solche begründen.[581] Die Detailtiefe der Aufgabenverteilung sollte in einem angemessenen Verhältnis zum Umfang der Verarbeitung sowie den damit für die betroffenen Personen verbundenen Risiken erfolgen.[582] Die Aufgaben sollten von der Stelle übernommen werden, welche am geeignetsten und effektivsten die Rechte und Pflichten umsetzen kann – die Aufgaben können dabei durchaus sehr ungleich verteilt sein.[583] Eine Pauschalübernahme sämtlicher Pflichten durch eine Stelle wird hingegen als nicht hinreichend transparent und konkret kritisiert.[584] Zudem muss das wesentliche der Vereinbarung der betroffenen Person zur Verfügung gestellt werden (Art. 26 Abs. 2 S. 2 DSGVO). Hierbei werden die Informationspflichten besonders hervorgehoben sowie der Fakt, dass es aus Betroffenensicht sehr nützlich ist, eine Anlaufstelle für die Geltendmachung der Betroffenenrechte zu haben – selbst wenn diese ungeachtet dieser Vereinbarung ihre Rechte gemäß Art. 26 Abs. 3 DSGVO gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.[585]

---

[580] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 7.

[581] *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 26 Rn. 22; *Lang,* in: Taeger/Gabel - DSGVO/BDSG Art. 26 Rn. 27; *Piltz,* in: Gola DS-GVO, Art. 26 Rn. 10: „Ein ‚Outsourcing' an allein auf dem Papier Verantwortliche ist nicht möglich."

[582] *Lang,* in: Taeger/Gabel - DSGVO/BDSG Art. 26 Rn. 32.

[583] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 42.

[584] *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit; *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 54. Vgl. auch: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 42. Manche Anforderungen treffen alle Verantwortlichen und können nicht auf einen delegiert werden.

[585] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 53.

Pflichten der DSGVO	Aufgabenverteilung zwischen gemeinsam Verantwortlichen
Festlegung Zwecke und Mittel der Verarbeitung	Zentraler Startpunkt für die Annahme einer gemeinsamen Verantwortlichkeit ist die Verfolgung gemeinsamer Zwecke durch gemeinsam festgelegte Mittel.
Rechtsgrundlagen, Umsetzung der Datenschutzgrundprinzipien	Bezüglich der Pflicht zur Umsetzung der Grundsätze aus Art. 5 DSGVO ist diese grundsätzlich nicht aufteilbar, sondern trifft alle Verantwortlichen gleichermaßen.[586] Fraglich ist, ob der Austausch von Daten zwischen den Verantwortlichen eine rechtfertigungsbedürftige Übermittlung darstellt.[587] Eine Privilegierung dürfte allerdings nicht bezweckt sein, sodass die Verantwortlichen für sämtliche Verarbeitungsschritte Rechtsgrundlagen vorweisen müssen.[588]
Informationspflichten	Bereitstellung der nach Art. 13 bzw. Art. 14 DSGVO erforderlichen Informationen gegenüber den betroffenen Personen
Dokumentationspflichten	Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO; ggf. Dokumentation von Einwilligungserklärungen
Datenschutzfreundliche Technikgestaltung, Datensicherheit und Datenschutz-Folgenabschätzung	Durchführung von Risikobeurteilungen, Umsetzung technischer und/oder organisatorischer Maßnahmen, Durchführung der DSFA
Umsetzung der Betroffenenrechte ▪ Auskunftsrecht ▪ Berichtigungsrecht ▪ Recht auf Löschung ▪ Recht auf Einschränkung der Verarbeitung ▪ Widerspruchs-/Widerrufsrecht ▪ Datenübertragbarkeit	Benennung eines/mehrerer Ansprechpartner für betroffene Personen. Nach Art. 26 Abs. 1 S. 3 DSGVO kann in der Vereinbarung zur gemeinsamen Verantwortlichkeit eine Anlaufstelle angegeben werden. Die betroffene Person kann ungeachtet dieser Vereinbarung ihre Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).
Meldepflichten	Meldung und Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten (Art. 33 f. DSGVO)
Bei Auftragsverarbeitung:	Auswahl und Kontrolle eines Auftragsverarbeiters
Bei Drittstaatentransfers:	Umsetzung der Anforderungen nach Kapitel V DSGVO

Tabelle 4 Überblick zur Aufgabenwahrnehmung bei gemeinsam Verantwortlichen

Hervorgehoben werden soll an dieser Stelle, dass auch ein Verstoß gegen Art. 26 DSGVO nach Art. 83 Abs. 4

[586] *Lang,* in: Taeger/Gabel - DSGVO/BDSG Art. 26 Rn. 31.; vgl. auch: *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit.
[587] *Piltz,* in: Gola DS-GVO, Art. 26 Rn. 8.
[588] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 62; *Bertermann,* in: Ehmann/Selmayr - DSGVO Art. 26 Rn. 11; *Spoerr,* in: BeckOK DatenschutzR Art. 26 Rn. 23; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 42.

Buchst. a DSGVO mit einem Bußgeld geahndet werden kann.[589] Zudem wären bei unzureichend konkretisierender Aufgabenzuweisung weitere Datenschutzverstöße zu befürchten, wenn die Verantwortlichen bestimmte Pflichten nicht oder nicht ausreichend umsetzen. Fraglich ist, welche Haftungsrisiken drohen, wenn einer der beteiligten Verantwortlichen seine zugewiesenen bzw. übernommenen Pflichten nicht erfüllt. Einerseits könnten mehrere Verantwortliche gesamtschuldnerisch haften, sodass sie nicht zur Entlastung auf den jeweils anderen nach der internen Verantwortungsverteilung verweisen können.[590] Andererseits könnte auch eine differenzierte Betrachtung angelegt werden, gerade wenn die Verantwortlichkeit nicht gleichwertig verteilt ist (bspw. ein Verantwortlicher hat keinen Zugang zu Daten), sodass eine wirksame Pflichtenverteilung auch gegenüber den Aufsichtsbehörden und potentiellen Sanktionen entlastend wirken würde.[591] Als Gegenargument kann ins Feld geführt werden, dass Verantwortliche die rechtskonforme Pflichtenumsetzung beim (Mit-)Verantwortlichen einfordern müssen.[592] Daher sollten ausdrückliche Regelungen über einen Ausgleich im Innenverhältnis in eine entsprechende Vereinbarung aufgenommen werden.

5.8.1.2 Anforderungen bei einer Auftragsverarbeitung (AV), Art. 28 und Art. 29 DSGVO

Eine AV liegt vor, wenn die Datenverarbeitung auf Weisung des Verantwortlichen erfolgt, was allerdings nicht unter dessen direkter Autorität oder Kontrolle meint.[593] Es bedeutet aber, dass der Auftragsverarbeiter in fremdem Interesse tätig wird. Die Rechtsgrundlage der Datenverarbeitung durch den Auftragsverarbeiter folgt aus der Beziehung des Verantwortlichen zur betroffenen Person, sofern der Auftragsverarbeiter die Daten nicht anders als auf Anweisung des für die Verarbeitung Verantwortlichen verarbeitet.[594]

> **Art. 28 Abs. 1 DSGVO** Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Art. 28 Abs. 1 DSGVO richtet sich zunächst an den Verantwortlichen, der dazu verpflichtet wird, nur mit „geeigneten“ Auftragsverarbeitern zu arbeiten. Somit normiert Art. 28 Abs. 1 DSGVO vor allem die Anforderungen, die der Verantwortliche an seine Auftragsverarbeiter zu stellen hat.[595] Demnach hat der Verantwortliche nicht nur eine Sorgfaltspflicht hinsichtlich der Auswahl eines geeigneten Auftragsverarbeiters, sondern muss auch während der Verarbeitung überprüfen, dass der Auftragsverarbeiter in DSGVO-konformer Weise die Verarbeitung durchführt.[596] Als hinreichen Garantien für die Einhaltung der Abs. 1 und Abs. 4 können laut Art. 28

[589] *Piltz,* in: Gola DS-GVO, Art. 26 Rn. 28; *Spoerr,* in: BeckOK DatenschutzR Art. 26 Rn. 27.
[590] *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 26 Rn. 22; *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 64.
[591] Vgl. *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 63 noch zur alten Rechtslage. Ähnlich wohl: *Jung/Hansch*, ZD 2019, 143 (144). Zur Störerauswahl: *Schwartmann/Burkhardt*, ZD 2021, 235 (237).
[592] Vgl. *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, S. 2; siehe auch zur Kontrollmöglichkeit der Aufsichtsbehörden: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 45.
[593] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 24.
[594] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 24; *Felber*, ZD 2018, 382 (385).
[595] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 27 ff.
[596] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 41; vgl. auch *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 7.

Abs. 5 die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO als Faktor herangezogen werden.

Eine Auftragsverarbeitung wird dann verneint, wenn der Auftragsverarbeiter sich eigene Wertungs- und Entscheidungsspielräume einräumt und seine Tätigkeit über reine Hilfsfunktionen für die Erfüllung der Zwecke des Auftraggebers hinausgeht.[597] Selbst bei einer Beauftragung einer externen Stelle soll keine Auftragsverarbeitung im datenschutzrechtlichen Sinne vorliegen, wenn diese eigenständig und ohne Vorgaben über technische und organisatorische Mittel der Datenverarbeitung entscheiden kann.[598] Auf die Rechtsnatur der Betrauung des Auftragsverarbeiters nach Zivilrecht kommt es dabei nicht an.[599] Ob eine Stelle eine Doppelfunktion als Verantwortlicher und Auftragsverarbeiter einnehmen kann, hängt davon ab, ob es sich um einen einheitlichen Vorgang handelt oder ob sich der Vorgang in verschiedene, rechtlich selbständig bewertbare Teile zerlegen lässt.[600] Die Entscheidung über den Verarbeitungszweck impliziert stets die datenschutzrechtliche Verantwortlichkeit.[601]

Auftragsverarbeitungsvertrag (AV-Vertrag): Art. 28 Abs. 3 DSGVO verpflichtet zum Abschluss eins AV-Vertrags. Zu diesen inhaltlichen Mindestanforderungen gehören:

- Festlegung von Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen;
- eine Verpflichtung des Auftragsverarbeiters nur auf dokumentierte Weisungen des Verantwortlichen personenbezogene Daten zu verarbeiten (Buchst. a),
- eine Verschwiegenheitsklausel (Buchst. b),
- die Verpflichtung alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zur Datensicherheit ergreifen (Buchst. c),
- die Einhaltung der Regelungen zur Subbeauftragung weiterer Unterauftragnehmer (Buchst. d),
- die Unterstützungspflicht bei Anträgen zur Geltendmachung von Betroffenenrechten durch geeignete TOM (Buchst. e),
- die Unterstützungspflicht zur Einhaltung der Art. 32- 36 DSGVO[602] (Buchst. f),
- zur Lösch- bzw. Rückgabepflicht (Buchst. g) und
- zum Nachweis der Einhaltung der Verpflichtungen aus Art. 28 DSGVO (Buchst. h).

Zusätzlich normiert Art. 28 Abs. 3 S.3 DSGVO eine Hinweispflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen, sofern er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen Datenschutzbestimmung verstößt.

---

[597] BGH, Urteil vom 13.7.2016 – IV ZR 292/14, Rn. 39; VGH München, Beschluss vom 26.09.2018 – 5 CS 18.1157, Rn. 16; VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 48. Zur Übertragbarkeit auf die DSGVO: *Felber*, ZD 2018, 382 (386).

[598] VGH München, Beschluss vom 26.09.2018 – 5 CS 18.1157, Rn. 16.

[599] BGH, Urteil vom 13.7.2016 – IV ZR 292/14, Rn. 39; VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 48.

[600] VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 49.

[601] Vgl. EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 68; *Felber*, ZD 2018, 382 (386).

[602] Art. 32 bis 36 DSGVO verpflichten den Verantwortlichen, für eine angemessene Sicherheit der Verarbeitung zu sorgen (Art. 32), ggf. etwaige Datenschutzverletzungen an die Aufsichtsbehörde zu melden (Art. 33) bzw. betroffene Personen von solchen Verletzungen zu benachrichtigen (Art. 34), vor risikoträchtigen Verarbeitungen eine Datenschutz-Folgeabschätzung durchzuführen (Art. 35) und schließlich in bestimmten Zweifelfragen die Aufsichtsbehörde zu konsultieren (Art. 36).

Unterbeauftragung: Art. 28 Abs. 2 DSGVO regelt, in welcher Form Auftragsverarbeiter Unteraufträge erteilen dürfen. Grundsätzlich können Berechtigungen zur Unterbeauftragung im AV-Vertrag geregelt werden. Eine vorherige Genehmigung des Unterauftrags ist jedoch laut Art. 28 Abs. 2 DSGVO erforderlich.[603] Das weitere Vorgehen sowie die Haftung für Unterauftragsnehmer regelt Art. 28 Abs. 4 DSGVO.

Unterstützung des Verantwortlichen: Art. 28 Abs. 3 DSGVO verpflichtet die Auftragsverarbeiter dazu, Verantwortliche bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Personen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Mittel zu unterstützen.[604] Unterstützungspflichten des Auftragsverarbeiters sind in den Art. 32 bis 36 DSGVO teilweise bereits normiert. Durch die Regelung wird sichergestellt, dass diese Pflichten auch vertraglich mit geregelt werden.[605] Diese vertraglichen Pflichten können über die gesetzlichen hinausgehen.[606] Sie sind allerdings nicht abdingbar. Im Hinblick auf die erforderlichen TOMs zur Gewährleistung der Datensicherheit muss geklärt werden, wer die Risikobewertung durchführt. Die Verantwortlichkeit für die Risikobewertung könnte beispielsweise Teil der vertraglichen Regelung sein, die Art. 28 Abs. 3 Buchst. f DSGVO vorsieht.[607] Damit Verantwortliche ihren Informations- und Auskunftspflichten nachkommen können, könnten sie Informationen vom Auftragsverarbeiter benötigen. Auch das Löschen, Berichtigen, Beschränken oder Übertragen muss durch den Auftragsverarbeiter technisch unterstützt werden, da der Verantwortliche ggfs. keinen Zugriff auf die Daten oder die entsprechenden Systeme hat, sofern die Daten beim Auftragsverarbeiter gespeichert werden.[608] Die Unterstützungspflicht muss technisch machbar sein und in das Aufgabenspektrum des Auftragsverarbeiters fallen.[609] Bei hohem Aufwand käme eine Vergütungsregelung je nach Aufwand in Betracht.[610]

Form: In Art. 28 Abs. 6-8 DSGVO ist die Verwendung von Standardvertragsklauseln geregelt. Art. 28 Abs. 9 DSGVO schreibt die Schriftform sowohl für den Auftragsvertrag als auch für mögliche Unteraufträge vor, wobei hierunter auch ein elektronisches Format fällt.[611]

[603] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 42.
[604] Eine ausführliche Übersicht über die Pflichten des Auftragsverarbeiters ist zu finden in: *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, Kap. 5 Rn. 8.
[605] Vgl. *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 28 Rn. 75; *Klug,* in: Gola DS-GVO, Art. 28 Rn. 7.
[606] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 72.
[607] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 73; *Witt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. 6 Maßnahmenübersicht und deren risikobasierte Bewertung bei der Auftragsverarbeitung Rn 1-4 bietet eine Übersicht über vertraglich regelbare Maßnahme zur Sicherung der Datenverarbeitung.
[608] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 70.
[609] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 70.
[610] *Bertemann,* in: Ehmann/Selmayr - DSGVO Art. 28 Rn. 27.
[611] Die Weisungen, auch mündliche, müssen dokumentiert sein und im Rahmen des Vertrags oder Rechtsinstruments konkret geregelt werden. Die Dokumentation der Weisungen kann in Textform im Sinne des 126b BGB oder in einem anderen elektronischen Verfahren, dass ein Mindestmaß an Manipulationsschutz aufbietet, erfolgen: *Bertemann,* in: Ehmann/Selmayr - DSGVO Art. 28 Rn. 3; *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 28 Rn. 99.

Folgen: Art. 29 DSGVO unterstreicht, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind. Art. 28 Abs. 10 DSGVO stellt klar, dass ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher gilt.

Praxistipp

Da AV-Verträge in der Praxis häufig auf Musterverträgen der Dienstleister beruhen, sollte besonders darauf geachtet werden, dass

- die Weisungsgebundenheit des Auftragsverarbeiters umfassend geregelt wird und
- dem Verantwortlichen hinreichend Kontrollbefugnisse eingeräumt werden.

Verarbeitet der Dienstanbieter personenbezogene Daten der Betroffenen auch zu eigenen Zwecken oder Zwecken Dritter (z. B. Verarbeitung von Daten zum Nutzerverhalten, Einsatz von Analysetools, Tracking zu Werbezwecken), liegt keine Auftragsverarbeitung vor

5.8.2 Dokumentation: Verarbeitungsverzeichnis

Im Hinblick auf die Rechenschaftspflicht sind Verantwortliche dazu angehalten alle Datenverarbeitungsprozesse in einem Verzeichnis der Verarbeitungstätigkeiten zu erfassen (Art. 30 DSGVO). Insbesondere die Dokumentation entsprechender Handlungsanweisungen, Betriebsvereinbarungen mithin alle organisatorischen Maßnahmen im Zusammenhang mit der Einführung und Nutzung von Kommunikations- und Kollaborationstools. Abschnitt IV der DSGVO gibt zudem Vorgaben, wann ein:e Datenschutzbeauftragte*r zu bestellen ist, welche Aufgaben diese:r erfüllt und wie seine/ihre Stellung aussieht. Ergänzt werden diese Vorschriften durch § 38 BDSG. Ausnahmen im Hinblick auf die Pflicht ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, gelten gemäß Art. 30 Abs. 5 DSGVO für:

- Unternehmen oder Einrichtung mit weniger als 250 Beschäftigten,
- Die vorgenommene Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen und / oder erfolgt nur gelegentlich,
- Keine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO und personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.

5.8.3 Meldepflichten: Data Breach Notification

Meldepflicht gegenüber Aufsichtsbehörden: Gemäß Art. 33 Abs. 1 DSGVO muss im Falle der Verletzung des Schutzes personenbezogener Daten der Verantwortliche diesen Vorfall unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Verletzung an seine zuständige Aufsichtsbehörde melden. Art. 55 DSGVO klärt, welche Aufsichtsbehörde zuständig ist. Nach seinem Wortlaut könnte „Verletzungen des Schutzes personenbezogener Daten“ jeden beliebigen Datenschutzverstoß umfassen – gemeint ist allerdings „*eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur*

Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“ (Art. 4 Nr. 12 DSGVO). [612] Die englische Bezeichnung „personal data breach“ ist insofern passender, da deutlich wird, dass es um sog. „Datenpannen“ geht, also primär sicherheitsbezogene Vorfälle.[613]

Nach Art. 33 Abs. 2 DSGVO muss der Auftragsverarbeiter entsprechend an den Verantwortlichen melden. Art. 33 Abs. 3 DSGVO benennt einen Mindestsatz an Informationen, die eine Meldung enthalten muss. Die Bereitstellung der Informationen ist auch schrittweise möglich (Art. 33 Abs. 4 DSGVO). Art. 33 Abs. 5 DSGVO verpflichtet zudem zur Dokumentation aller im Zusammenhang mit dem Vorfall stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen, sodass der Aufsichtsbehörde eine Überprüfung der Einhaltung der Data-Breach-Notification-Vorgaben möglich ist.

Ausnahmen von der Meldepflicht: Von der Meldepflicht ausgenommen sind Verletzungen des Schutzes personenbezogener Daten, die „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen“. Hierbei ist gemeint, dass sich das Risiko voraussichtlich nicht realisiert: besteht kein hohes oder normales Risiko, sondern nur ein geringes Risiko, muss nicht gemeldet werden.[614]

Information betroffener Personen: Darüber hinaus sind unverzüglich alle betroffenen Personen gemäß Art. 34 Abs. 1 DSGVO zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Auch in diesem Zusammenhang ist wieder die Risikobeurteilung elementar.[615] Diese Benachrichtigung muss:

- In klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten umschreiben (Art. 34 Abs. 2 DSGVO) und
- Informationen zum Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen enthalten (Art. 34 Abs. 2 i.V.m. Art. 33 Abs. 3 Buchst. b, c und d DSGVO).

Art. 34 Abs. 3 DSGVO enthält wiederum Ausnahmen von der Benachrichtigungspflicht bei:

- Ergreifen geeigneter technischer und organisatorischer Sicherheitsvorkehrungen, die Daten unzugänglich machen (präventiv),[616]
- Sicherstellung durch nachfolgende Maßnahmen, dass ein hohes Risiko aller Wahrscheinlichkeit nicht mehr besteht,[617] oder

[612] *Bieker u. a.*, DuD 2018, 492 (496).
[613] *Bieker u. a.*, DuD 2018, 492 (496).
[614] *Bieker u. a.*, DuD 2018, 492 (496); vgl. auch *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 18 ff.
[615] Zur Risikobeurteilung im Rahmen der datenschutzfreundlichen Technikgestaltung siehe Abschnitt 2.4.4.2.1.
[616] *Jandt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 34 Rn. 14; vgl. auch *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 18 zur Frage der Meldepflicht bei verschlüsselten Daten.
[617] Zur Auslegung: *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 22 ff.

- Wenn die Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde.[618] Die Einzelbenachrichtigung kann dann durch eine öffentliche Bekanntmachung oder vergleichbar wirksam informierende Maßnahme ersetzt werden.

Der EDSA stellt in seinen Guidelines zur Data-Breach-Notification eine Übersicht bereit:[619]

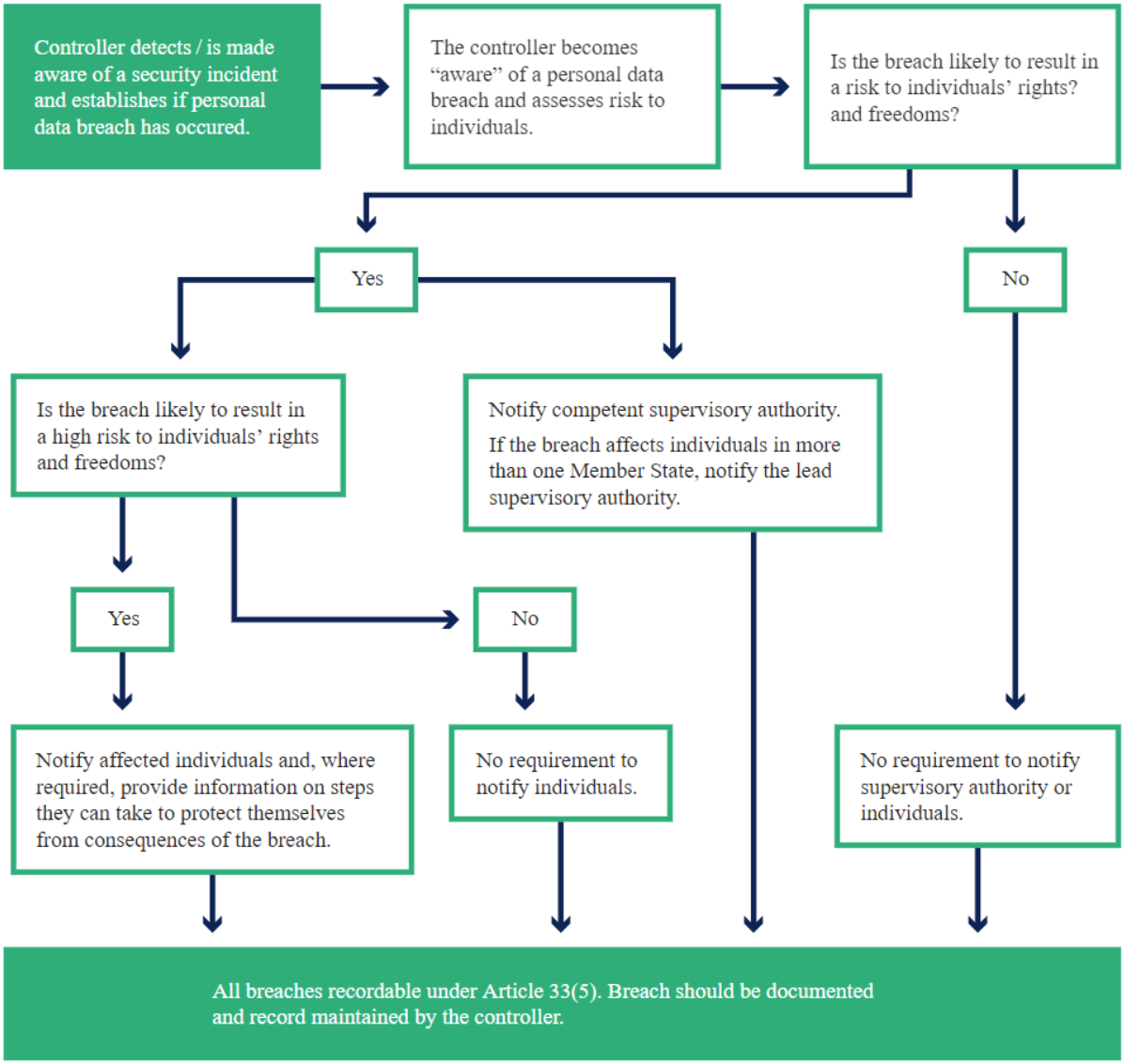


Abbildung 15 Flowchart zu Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO des EDSA

[618] Zur Unverhältnismäßigkeit des Aufwands: *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 22; *Jandt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 34 Rn. 15a m.w.N.

[619] *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 30.

5.8.4 Hilfestellungen zur Umsetzung der Rechenschaftspflicht

5.8.4.1 Datenschutzmanagementsysteme (DSMS)

Zur besseren Organisation, gerade bei komplexen Verarbeitungsketten und/oder mehreren Beteiligten, bieten sich DSMS an, um die Rechenschaftspflicht umzusetzen. Als weitere Vorteile werden Potentiale zur Einsparung digitaler wie analoger Speicherplätze genannt (z. B. durch Vermeidung von Doppelspeicherungen, übersichtliche Speicherpfade oder strukturierte Ablagesysteme).[620] Compliance-Management-Systeme (CMS) sowie Information Security Management Systems (ISMS) sind im unternehmerischen Alltag bereits etabliert. Durch die Rechenschaftspflicht der DSGVO steigt die Bedeutung, diese Ansätze um DSMS zu erweitern.[621] Dieses sollte Datenschutzleitlinien mit klaren Vorgaben zu Aufgaben und Rollen, Berichtswesen, Prozessgestaltung, etc., spezifizierende Datenschutzrichtlinien mit konkreten Vorgaben zu einzelnen Maßnahmen und Templates, Arbeitsanweisungen, Schulungsmaßnahmen und Audits umfassen.[622]

5.8.4.2 Zuordnung von Verantwortlichkeit innerhalb eines Unternehmens

Vor der Inbetriebnahme einer KI-Lösung sollten Rollen und Verantwortlichkeiten im Unternehmen klar definiert werden, sofern dieses die datenschutzrechtliche Verantwortlichkeit trägt.[623] Sind im Rahmen von Unternehmensverbünden oder Projekten mit anderen Partnern mehrere bzw. zahlreiche Personen beteiligt, kann es mitunter Schwierigkeiten bereiten, Verantwortlichkeiten eindeutig zuzuweisen, wobei sich Unternehmen regelmäßig die Handlungen ihrer Beschäftigten zurechnen lassen müssen. In anderen Kontexten wurden bereits Verantwortlichkeitsmatrizen wie die RACI[624] bzw. RASCI[625]-Matrix entwickelt.[626] Dabei handelt es sich um eine Technik zur Analyse und Darstellung von Verantwortlichkeiten. Diese Techniken könnten auch eingesetzt werden, um bei der Umsetzung der datenschutzrechtlichen Rechenschaftspflicht zu unterstützen. [627] Hierbei ist natürlich zu berücksichtigen, dass die Modelle ggf. an gesetzliche Vorgaben angepasst danach werden müssen, welche sich auf die Rollen auswirken, die im Unternehmen die Durchführungsverantwortung („*Responsibility*“) und welche die Gesamtverantwortung („*Accountability*“) tragen, wer gesetzlich verpflichtend beratend zu konsultieren ist (Datenschutzbeauftragter, Betriebsrat) und wie Einzelprozessschritte zu dokumentieren sind (Verfahrensverzeichnisse nach Art. 30 DSGVO).[628]

5.8.5 Rechtsfolgen bei Verstößen

Werden Aufsichtsbehörden Verstöße gegen die Datenschutzvorgaben bekannt, gewährt ihnen Art. 58 DSGVO unterschiedliche Befugnisse beispielsweise zur Ergreifung von Maßnahmen, die Abhilfe schaffen sollen, als auch eine Geldbuße gemäß Art. 83 DSGVO zu verhängen (Art. 58 Abs. 2 Buchst. i DSGVO). Hierbei muss der Schadensersatzanspruch aus Art. 82 DSGVO von den Geldbußen durch die Behörden nach Art. 83 DSGVO un-

[620] *Lurtz*, ZD-Aktuell 2021, 05269.
[621] *Jung*, ZD 2018, 208 (208 ff.).
[622] *Jung*, ZD 2018, 208 (212 f.).
[623] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 8.
[624] RACI steht für die jeweiligen Anfangsbuchstaben der Worte Responsible, Accountable, Consulted, Informed.
[625] Die Abkürzung RASCI leitet sich aus Responsible, Accountable, Supported, Consulted und Informed ab.
[626] *Jung/Hansch*, ZD 2019, 143 (143).
[627] *Jung/Hansch*, ZD 2019, 143 (143).
[628] *Jung/Hansch*, ZD 2019, 143 (144).

terschieden werden. Der EDSA veröffentlichte im Frühling 2022 Guidelines über die Berechnung von Bußgeldern unter der DSGVO.[629]

Geldbußen: Allgemeine Bedingungen für das Verhängen von Bußgeldern sind in Art. 83 Abs. 1-3 DSGVO geregelt: Sanktionen sind im Einzelfall so zu bemessen, dass sie wirksam, verhältnismäßig und abschreckend sind. Sie können parallel zu anderen Maßnahmen verhängt werden. Obergrenze des Gesamtbetrags soll bei Verstößen gegen mehrere Bestimmungen durch gleiche bzw. miteinander verbundene Verarbeitungsvorgänge (Tateinheit) die Sanktion für den schwerwiegendsten Verstoß sein. Die Höhe der möglichen Sanktionen hängen dabei von der Art des Verstoßes sowie der Norm gegen welche verstoßen wurde ab (vgl. Tabelle 5).[630]

Norm	Höhe	Verstoß gegen
Art. 83 Abs. 4 DSGVO	bis zu 10.000.000 € oder 2 % des Umsatzes	Art. 8, 11, 25 bis 39, 42 und 43 für Verantwortliche und Auftragsverarbeiter
Art. 83 Abs. 5 DSGVO	bis zu 20.000.000 € oder 4 % des Umsatzes	Grundsätze gemäß Art. 5, 6, 7 und 9 Betroffenenrechte nach Art. 12 bis 22 Drittlandübermittlung nach Art. 44 bis 49 Pflichten nach Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden Nichtbefolgung Anweisungen Aufsichtbehörde
Art. 83 Abs. 6 DSGVO	bis zu 20.000.000 € oder 4 % des Umsatzes	Nichtbefolgung einer Anweisung einer Aufsichtsbehörde gemäß Art. 58 Abs. 2 DSGVO

Tabelle 5 Sanktionsstufen

Mit unabhängig betriebenen Informationsportalen wie dem GDPR Enforcement Tracker[631], dem DSGVO-Portal[632] oder dem Projekt29[633] werden aktuelle Sanktionen EU-weit veröffentlicht.

Schadensersatz: Die Schadensersatzansprüche werden in Art. 82 DSGVO konkretisiert:

- Anspruchsberechtigt ist *jede* Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist (Abs. 1). Umstritten ist, ob dies auf betroffene Personen i.S.d. Art. 4 Nr. 1 DSGVO[634] oder natürliche Personen[635] beschränkt ist. In der Praxis dürften Schäden ohnehin zumeist bei der betroffenen Person entstehen.
- Anspruchsgegner sind Verantwortlicher oder Auftragsverarbeiter:
  - Jeder beteiligte Verantwortliche haftet für durch Verstöße verursachte Schäden (Abs. 2 S. 1)

[629] *European Data Protection Board*, Guidelines 04/2022 on the calculation of administrative fines under the GDPR.
[630] Für eine vollständige Übersicht inkl. Straftatbestände und Folgen siehe: https://www.datenschutz.org/dsgvo-bussgeld/#bkat [letzter Abruf 28.07.2021].
[631] https://www.enforcementtracker.com/, betrieben durch die CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB.
[632] https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php, betrieben durch die Compliance Essentials GmbH.
[633] https://www.projekt29.de/, Projekt 29 GmbH & Co. KG.
[634] So: *Gola/Piltz,* in: Gola DS-GVO, Art. 82 Rn. 10.
[635] So: *Bergt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 82 Rn. 13; *Moos/Schefzig,* in: Taeger/Gabel - DSGVO/BDSG Art. 82 Rn. 17.

  - Auftragsverarbeiter haften nur für Verletzung der ihnen speziell auferlegten Pflichten / Anweisungen der Verantwortlichen (Abs. 2 S. 2)
- Die Beweislast zum Nachweis eines fehlenden Verschuldens trägt der Verantwortliche / Auftragsverarbeiter (Abs. 3)
- Bei mehreren Verantwortlichen / Auftragsverarbeitern liegt eine gesamtschuldnerische Haftung vor (Abs. 4). Abs. 5 DSGVO regelt insoweit die Möglichkeit des Rückgriffsanspruchs der weiteren Haftungsschuldner, wenn einer für den gesamten Schaden aufgekommen ist.[636]

Daneben können Ansprüche auf Unterlassung und Schadensersatz aus Verstoß gegen arbeitsvertragliche Pflichten gegenüber den Beschäftigten sowie aus dem Deliktsrecht wegen Verletzung des Persönlichkeitsrechts treten (§§ 823 Abs. 1, 1004 BGB).[637]

Strafbarkeit: Datenschutzverletzungen können zudem zu Strafverfahren führen (vgl. § 42 BDSG).[638] Schwere Verstöße können laut § 42 BDSG als Antragsdelikte strafrechtlich verfolgt werden. Hierzu zählt beispielweise die unberechtigte, wissentliche Weitergabe von personenbezogenen Daten einer großen Anzahl von Personen an Dritte.

Haftung der Leitungsorgane: Haftet das Unternehmen als juristische Person für Datenschutzverstöße, können unter Umständen auch die innerhalb des Unternehmens verantwortlichen Personen für das fahrlässige oder vorsätzliche Unterlassen von Aufsichtsmaßnahmen mit ihrem Privatvermögen haften (vgl. §§ 130, 9 OWiG).[639] Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen (§ 130 Abs. 1 S. 2 OWiG).

Sonstige Folgekosten: Entsprechende Geldbußen können darüber hinaus Folgekosten verursachen: Neben der kurzfristigen Einholung von kostenintensiven Datenschutz- und ggf. PR-Strategien, kann die Eintragung in das Gewerbezentralregister gemäß § 149 Abs. 2 Nr. 3 und 4 GewO Einfluss auf die Kreditwürdigkeit des Betriebs haben.[640]

5.9 Zwischenergebnis zur Umsetzung der Datenschutzgrundprinzipien und Bedeutung für die KI-Systemnutzung

Die Datenschutzgrundprinzipien bieten einen guten Rahmen zur Erfassung der wesentlichen Pflichten. Starten sollten Verantwortliche mit einer genauen Definition der verfolgten Zwecke. Daraus leitet sich die einschlägige Rechtsgrundlage, die Risikobewertung im Hinblick auf Datenminimierung und Datensicherheit sowie das Löschkonzept ab. In organisatorischer Hinsicht ist sicherzustellen, dass u.a. Auskunftsersuchen, Berichtigungs- und Löschanfragen rechtzeitig erfüllt werden können. Alle wesentlichen Entscheidungen sollten nachvollziehbar dokumentiert werden.

[636] Zur Haftung als Gesamtschuldner: *Gola/Piltz,* in: Gola DS-GVO, Art. 82 Rn. 6 ff.
[637] BAG, Urteil vom 12. 9. 2006 - 9 AZR 271/06, Rn. 21.
[638] *Lurtz*, ZD-Aktuell 2021, 05269.
[639] *Faas*, ArbRAktuell 2018, 594 (595).
[640] *Lurtz*, ZD-Aktuell 2021, 05269.

6 Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Abbildung 16 gibt einen Überblick über potentiell einschlägige Rechtsgrundlagen. Besonderheiten bestehen bei der Verarbeitung besonderer Kategorien personenbezogener Daten (hierzu Abschnitt 10.1). Bei Datenverarbeitungen im Rahmen des Anwendungsbereichs des die ePrivacy-Richtlinie umsetzenden TTDSG, werden die Vorgaben der DSGVO teilweise überlagert. Aufgrund von Öffnungsklauseln bestehen Besonderheiten im Beschäftigungsverhältnis. Ebenso finden sich im Bundes- und Landesdatenschutzrecht Regelungen zur Forschung. Rechtliche Verpflichtungen und öffentliche Aufgaben können sich aus Unionsrecht oder dem Recht der Mitgliedstaaten ergeben.

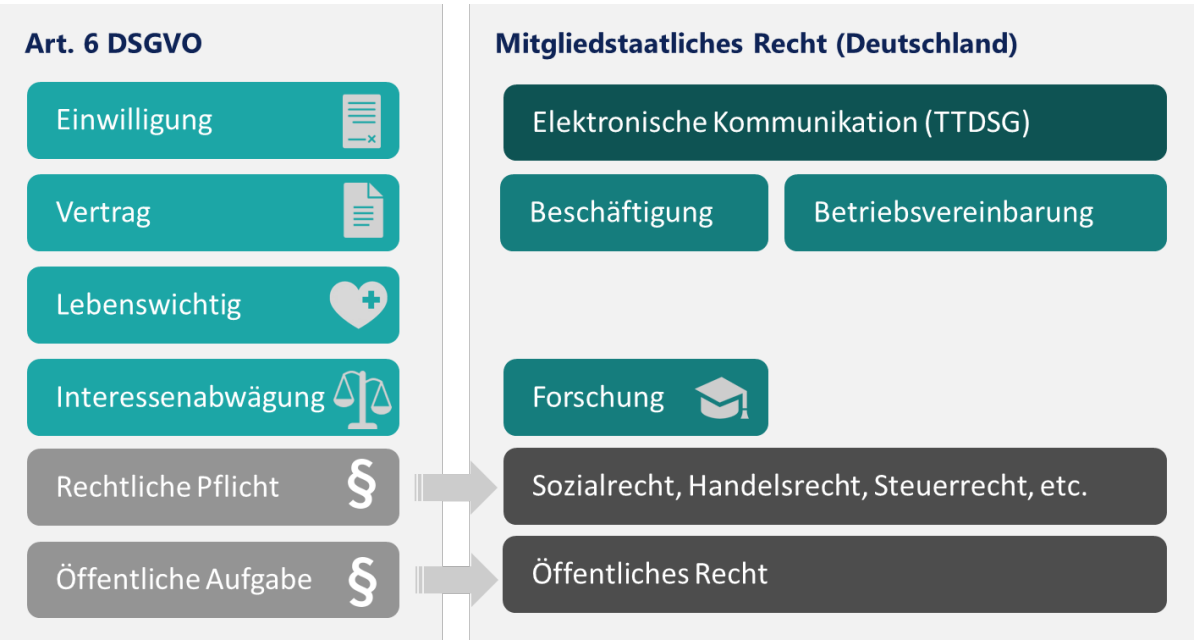


Abbildung 16 Überblick über relevante Rechtsgrundlagen

6.1 Einwilligung

Die Einwilligung ist in Art. 6 Abs.1 DSGVO an erster Stelle der Erlaubnistatbestände als Ausdruck datenschutzrechtlicher Selbstbestimmung normiert.[641] Damit sollte die betroffene Person in die Lage versetzt werden, privatautonom über das „Ob“ und „Wie“ der Verarbeitung ihrer personenbezogenen Daten zu bestimmen. Der Grundgedanke besteht darin, dass demjenigen kein Unrecht geschieht, der „sich mit klarem Kopf, hinreichend informiert und ohne Zwang“ eine bestimmte Datenverarbeitung ausgesucht hat.[642] Entsprechend müssen aber auch die Anforderungen an eine wirksame Einwilligung erfüllt sein, um legitimierend zu wirken.

Art. 6 Abs. 1 Buchst. a DSGVO Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

Art. 4 Nr. 11 DSGVO „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise

[641] *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 21. Aus dieser Stellung folgt allerdings keine Vorrangwirkung, a.A. *Sattler*, JZ 2017, 1036 (1040).
[642] *Samardzic/Becker*, EuZW 2020, 646 (649).

> und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Die Wirksamkeitsvoraussetzungen einer Einwilligung sind in Art. 4 Nr. 11, Art. 6 Abs. 1 Buchst. a und Art. 7 Abs. 1-4 DSGVO geregelt. Danach müsste eine wirksame Einwilligung folgende Kriterien erfüllen:

6.1.1 Bestimmt, spezifisch und unmissverständlich

Die betroffene Person muss ihre Einwilligung „für einen oder mehrere Zwecke“ geben. Diese Zwecke müssen so präzise wie möglich beschrieben werden. Eine pauschale Einwilligung ist stets unwirksam.[643] Die betroffene Person muss nach Ansicht des EDSA in Bezug auf jeden dieser Zwecke eine Wahlmöglichkeit haben.[644] Dies erfordert:

- Spezifizierung des Zwecks als Schutz vor schleichender Funktionserweiterung,
- Granularität bei Einwilligungsanfragen und
- Klare Trennung von Informationen, die sich auf die Einwilligung beziehen, von Informationen über andere Angelegenheiten.[645]

Selbst bei komplexen „Big-Data-Analysen“ müssen die Zwecke der Datenverarbeitung so weit wie möglich zu konkretisiert werden und Einwilligung zu verschiedenen Verarbeitungsvorgängen möglich sein, d. h. die Einwilligungserklärung muss insgesamt hinreichend granular aufgebaut sein.[646]

6.1.2 Informiert

Die Einwilligung muss auch „in informierter Weise“ abgegeben werden. D. h. vor der Datenverarbeitung muss die betroffene Person wissen und verstehen, auf welche personenbezogene Daten sich die Einwilligung bezieht, was mit den Daten geschehen soll und wer für die Datenverarbeitung verantwortlich ist (ErwGr. 42 S. 4 DSGVO).[647] Dafür muss die Datenschutzerklärung in verständlicher und leicht zugänglicher Form und in klarer, einfacher Sprache erfolgen. Betrifft die Datenschutzerklärung mehrere Sachverhalte, sind die jeweilige Sachverhalte eindeutig voneinander zu unterscheiden, Art. 7 Abs. 2 DSGVO. In der Praxis gilt allerdings zu bemängeln, dass dies gerade bei umfangreicher Datenverarbeitungspraxis zu großer Informationsflut

[643] *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 62; *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 8; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 39; *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 76.; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 78. Zu Ausnahmen in der Forschung vgl. ErwGr. 33.
[644] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 13.
[645] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 14.
[646] *Gausling*, DSRITB 2018, 519 (531).
[647] *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 34.

führt.[648] Insofern werden auch Zweifel geäußert, ob das Anliegen der Informiertheit so erreicht wird.[649] Der EDSA nennt die folgenden Angaben als Mindestset an Informationen:[650]

- Identität des Verantwortlichen
- Zweck der Datenverarbeitung
- Welche (Art von) Daten erfasst sind
- Bestehen des Widerrufsrechts
- Sofern einschlägig: Informationen über automatisierte Entscheidungsfindung
- zu den möglichen Risiken von Datenübermittlungen (auch aufgrund des Fehlens eines Angemessenheitsbeschlusses oder geeigneter Garantien)

Ziel der Information ist es, dass die betroffene Person die betreffenden Verarbeitungsvorgänge wirklich verstehen kann.[651] Ob dies angesichts der viel bemängelten Intransparenz von KI-Systemen tatsächlich möglich ist, hängt auch davon ab, wie genau über dessen Funktionsweise informiert werden muss. Insofern gelten die im Rahmen der Transparenzpflichten dargestellten Diskussionen zum „Recht auf Erklärbarkeit“ auch in diesem Kontext (vgl. Abschnitt 5.2.2.3).

6.1.3 Durch eine aktive Handlung

Für eine wirksame Einwilligung ist stets eine Erklärung oder eine sonstige eindeutig bestätigende Handlung erforderlich.[652] ErwGr. 32 S. 3 erläutert diese Voraussetzung dahingehend, dass Stillschweigen oder vorangekreuzte Kästchen nicht genügen. Auch der EuGH stellte klar, dass nur ein *Opt-In* eine wirksame Einwilligung darstellt – ein *Opt-Out* hingegen nicht.[653]

Die DSGVO schreibt dabei keine bestimmte Form für das Erteilen einer Einwilligung vor.[654] ErwGr. 32 S. 1 stellt sogar die elektronische und mündliche Erklärung der Schriftform gleich. Der Verantwortliche hat also grundsätzlich eine freie Auswahl, welches Formverfahren er anwenden möchte, trägt aber die Nachweispflicht dafür, dass eine wirksame Einwilligung der betroffenen Person vorliegt, Art. 7 Abs. 1 DSGVO.[655] Daher wird zu Dokumentationszwecken von konkludenten oder mündlichen Einwilligungen zumeist eher abgeraten – auch wenn diese grundsätzlich wirksam wären.[656]

6.1.4 Freiwillig

Eine wirksame Einwilligung muss freiwillig erfolgen, d. h. ohne jeden Zwang oder Druck.[657] Dies ist dann nicht

[648] *Samardzic/Becker*, EuZW 2020, 646 (651). Zu Optionen gestufter Informationskonzepte: *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 40. Negativbeispiel bei: LG Frankfurt, Urteil vom 10.06.2016 – 2-3 O 364/15.
[649] *Hermstrüwer*, Informationelle Selbstgefährdung, S. 282 ff.; *Wagner*, Datenökonomie und Selbstdatenschutz, S. 354; vgl. auch zur Kosten-Zeitaufwand-Relation: *McDonald/Cranor*, ISJLP 2008, 543; *Acquisti/Grossklags*, IEEE Security and Privacy Magazine 2005, 26.
[650] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 15.
[651] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 16.
[652] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 18.
[653] EuGH, Urteil vom 1. Oktober 2019, Az. C-673/17 – Planet49.
[654] EuGH, Urteil vom 1. Oktober 2019, Az. C-673/17 – Planet49; *Ziebarth/Elsaß*, ZUM 2018, 578 (579).
[655] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 22.
[656] *Steege*, MMR 2019, 509 (511).
[657] *Stemmer,* in: BeckOK DatenschutzR Art. 7 Rn. 39; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 26 f. *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 21.

der Fall, wenn die betroffene Person faktisch keine andere Wahl hat, als der Datenverarbeitung zuzustimmen (vgl. ErwGr. 42 S. 5). Um in den Genuss einer Dienstleistung oder einer anderen vertraglichen Leistung zu kommen, könnte oftmals keine realistische Möglichkeit bestehen, die Einwilligung zu verweigern oder zurückzuziehen.[658] Ebenso übermäßige Anreize können die Freiwilligkeit gefährden.[659] Eine wirksame Einwilligung ist auch zu verneinen, wenn die Beziehung zwischen der betroffenen Person und dem Verantwortlichen von einem klaren Ungleichgewicht geprägt ist und deshalb die Einwilligung mutmaßlich unfreiwillig erfolgte.[660] Eine Unfreiwilligkeit kann laut ErwGr. 43 insbesondere in folgenden Fällen vorliegen:

Machtasymmetrien	Pauschaleinwilligung	Kopplungsverbot
Es besteht ein klares Ungleichgewicht zwischen Verantwortlichem und betroffener Person. Es handelt sich bei dem Verantwortlichen um eine Behörde.	Es ist nicht möglich eine gesonderte Einwilligung in verschiedene Verarbeitungsvorgänge zu geben, obwohl dies im Einzelfall angebracht wäre.	Die Einwilligung ist Bedingung für einen Vertrag (einschließlich einer Dienstleistung), für deren/dessen Erfüllung die Datenverarbeitung nicht erforderlich ist

Abbildung 17 Beispiele für Unfreiwilligkeit der DSGVO

Machtasymmetrien: Explizit genannt werden Behörden, da im Bürger-Staat-Verhältnis zu vermuten ist, dass Bürger*innen bei behördlichen Maßnahmen kaum ausreichende Entscheidungsspielräume verbleiben.[661] Die Einwilligung ist zwar nicht generell ausgeschlossen, es besteht aber ein erhöhter Prüfungs- und Begründungsaufwand.[662] Typische Konstellationen sind Monopolstellungen.[663] Besondere Abhängigkeiten bestehen zudem bei wichtigen Leistungen, wie im Bereich der Daseinsvorsorge.[664] Eine weitere Unsicherheit besteht im Hinblick auf die Freiwilligkeit im Arbeitsverhältnis.[665] Zwar hatte die EU-Kommission die Einwilligungsmöglichkeit im Arbeitsverhältnis in ihrem DSGVO-Entwurf noch ausgeschlossen.[666] Diese Einschränkung wurde allerdings für die finale Fassung gestrichen. Nichtsdestotrotz werden von Arbeitgeber*innen gewünschte Datenverarbeitungen als typische die Entschließungsfreiheit hemmende Konstellationen eines

[658] *Stemmer,* in: BeckOK DatenschutzR Art. 7 Rn. 40; *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 7 Rn. 14.
[659] LG Stuttgart, Urteil vom 13. August 1998 – 17 O 329/98 –, Rn. 30; offen gelassen OLG Stuttgart, Urteil vom 27. November 1998 – 2 U 111/98 –, Rn. 34; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 15, 82 ff. Siehe auch zur sittenwidrigen Kopplung von Gewinnspielen mit dem Warenabsatz aufgrund psychischen Kaufzwangs: BGH, Urteil vom 05. Februar 1998 – I ZR 151/95 – Rubbelaktion, Rn. 15; BGH, Urteil vom 16. März 1989 – I ZR 241/86 – Gewinnspiel, Rn. 44; BGH, Urteil vom 19. Dezember 1975 – I ZR 120/74 – Versandhandels-Preisausschreiben, Rn. 31.
[660] Statt vieler: *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 7 Rn. 17.
[661] Differenzierend zwischen Eingriffsverwaltung und schlicht-hoheitlichem Handeln: *Samardzic/Becker*, EuZW 2020, 646 (652).
[662] Statt vieler: *Samardzic/Becker*, EuZW 2020, 646 (652).
[663] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 7 Rn. 17.
[664] Vgl. zur Forderung einer eDaseinsvorsorge: *Luch/Schulz*, MMR 2009, 19. Für eine Art „soziale Grundversorgung“: *Kamp/Rost*, DuD 2013, 80 (82).
[665] *Samardzic/Becker*, EuZW 2020, 646 (652); für Einwilligungsmöglichkeiten: *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[666] ErwGr. 34 in: EU-Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Brüssel, den 25.1.2012, KOM (2012) 11 final.

Machtungleichgewichts genannt.[667] Der deutsche Gesetzgeber hat diese Frage im Rahmen der Öffnungsklausel des Art. 88 DSGVO für den Bereich des Beschäftigungsverhältnisses spezifisch in § 26 Abs. 2, 3 BDSG adressiert (siehe hierzu ausführlich in Abschnitt 8.4). Aber auch sozialer Druck (bspw. zur Mithilfe bei der Eindämmung einer Pandemie) kann zu faktischen Zwängen führen.[668] Ebenso sollten Netzwerkeffekte und Lock-In-Effekte gerade im Bereich sozialer und/oder beruflicher Interaktion nicht unterschätzt werden.[669] Auch solche Zwangslagen angemessen zu berücksichtigen, erscheint aus verfassungsrechtlicher Sicht geboten.[670]

Pauschaleinwilligungen: Der Grundsatz der „differenzierten Einwilligung" gebietet es, dass mehrere voneinander getrennte Datenverarbeitungsvorgänge nicht lediglich unter eine pauschale Einwilligungsoption gestellt werden dürfen.[671] Ist die getrennte Einwilligungsmöglichkeit in verschiedenen Datenverarbeitungsvorgängen nicht möglich, obwohl es im konkreten Kontext angebracht wäre, wird das Fehlen der Freiwilligkeit vermutet.[672]

Kopplungsverbot: Besonders umstritten ist im Zusammenhang mit der Auslegung des Merkmals der Freiwilligkeit das in Art. 7 Abs. 4 DSGVO normierte sog. „Kopplungsverbot".[673] Dieses besagt, dass bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Folglich handelt es sich bereits dem Wortlaut nach nicht um ein Verbot im engeren Sinne.[674] Nichtsdestotrotz plädiert u.a. der EDSA für die Annahme einer vergleichbaren Wirkung.[675] In der Gesamtschau mit den ErwGr. 42, 43 sei praktisch ein Verbot beabsichtigt. [676] Gefordert wird, dass jede Art von Nachteil berücksichtigungsfähig sein sollte, unerheblich, ob es sich um einen materiellen oder immateriellen Nachteil handelt.[677] Daraus sei ein *Regel-Ausnahme-Verhältnis* dergestalt zu entnehmen, dass eine Vermutung der Unfreiwilligkeit im Fall einer Kopplung als Regel gleichwohl die Möglichkeit der Einwilligung in vertragsfremde Zwecke als Ausnahme nicht vollständig ausschließt.[678]

---

[667] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 7; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 27.

[668] *Samardzic/Becker*, EuZW 2020, 646 (652).

[669] Zu Netzwerkeffekten: *Monopolkommission*, Wettbewerb 2018, S. 243; *Monopolkommission*, Sondergutachten 68: Wettbewerbspolitik: Herausforderung digitale Märkte, S. 33; zu den Nutzungszahlen siehe: *Engels*, Datenschutzpräferenzen von Jugendlichen in Deutschland, S. 10.

[670] *Samardzic/Becker*, EuZW 2020, 646 (652).

[671] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 12; *Krohm*, ZD 2016, 368 (373).

[672] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 12; *Krohm*, ZD 2016, 368 (373).

[673] Zum Streit siehe: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 312 ff.

[674] *Brockmeyer*, ZD 2018, 258 (262); *Dammann*, ZD 2016, 307 (311); *Engeler*, ZD 2018, 55 (58); *Franzen,* in: Franzen/Gallner/Oetker, EuArbR Art. 7 DS-GVO Rn. 9; *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Heckmann/Paschke,* in: Ehmann/Selmayr - DSGVO Art. 7 Rn. 95; *Kugelmann*, DuD 2016, 566 (567); *Schantz*, NJW 2016, 1841 (1845); *Schätzle*, PinG 2017, 203 (205); *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 22; *Spindler*, JZ 2016, 805 (807); *Wybitul u. a.*, ZD 2017, 503 (507); *Schneider*, Datenschutz, S. 162.

[675] *Albrecht*, CR 2016, 88 (91); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 71 Rn. 44; *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 8f.; *Dammann*, ZD 2016, 307 (311); *Härting*, CR 2016, 735 (739); *Härting*, Datenschutz-Grundverordnung, S. 96 Rn. 392; *Krauß u. a.*, DuD 2017, 217 (219); *Krönke*, Der Staat 2016, 319 (327); *Krohm*, ZD 2016, 368 (373).

[676] *Dammann*, ZD 2016, 307 (311); so wohl im Ergebnis auch: *Gierschmann*, ZD 2016, 51 (54); *Wybitul*, ZD 2016, 203 (205); *Wybitul*, BB 2016, 1077 (1081).

[677] *Härting*, Datenschutz-Grundverordnung, S. 97 Rn. 398; *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 10.

[678] ÖOGH, Urteil vom 31.8.2018 – 6 Ob 140/18h, Rn. 46, ZD 2019, 72 (73); *Albrecht*, CR 2016, 88 (91); *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 9; *Ernst*, ZD 2017, 110 (112); *Härting*, CR 2016, 735

> **ErwGr. 42 S. 5 DSGVO** Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Der Gegenansicht nach handelt es sich lediglich um eine Auslegungshilfe, da sich ein striktes Kopplungsverbot in den Verhandlungen zur DSGVO eben nicht durchgesetzt hätte.[679] Dabei wird u. a. vertreten, dass die Erwägungsgründe restriktiv auszulegen seien, denn ein Nachteil bei Verweigerung oder Widerruf der Einwilligung könne nur bei schwerwiegenden Folgen, aber nicht bei bloßen Unannehmlichkeiten wie der Nichtgewährung von Preisnachlässen oder privatautonomer Ablehnung eines Vertragsschlusses angenommen werden – jedenfalls sofern keine monopolartigen Strukturen oder ein Fall der Daseinsvorsorge gegeben sei.[680] Somit müssten bei wertender Betrachtung entsprechende Drucksituation in die Beurteilung mit einbezogen werden.[681] Der Schutzzweck der Regelung greife erst bei Nachteilen „von gewissem Gewicht“,[682] dem Ausnutzen einer „starken Position“,[683] der Vorenthaltung einer informatorisch-kommunikativen Grundversorgung[684] oder „sachfremde“ Kopplungen.[685] Eine freie Wahl könne aber auch bei Verzicht auf einen Dienst ausgeübt werden.[686] Eine Kommerzialisierung der Einwilligung in Form der Gegenleistung für eine vermeintlich kostenlose Leistung solle weiterhin möglich bleiben, soweit die Wahl dieses Vertragsmodells freiwillig erfolge.[687]

6.1.5 Widerrufbar

Gemäß Art. 7 Abs. 3 S. 1 DSGVO haben betroffene Personen das Recht, jederzeit ihre Einwilligung zu widerrufen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Ferner ist die betroffene Person vor Abgabe der Einwilligung über ihr Widerrufsrecht zu belehren, Art. 7 Abs. 3 S. 3 DSGVO.

(739); *Härting*, Datenschutz-Grundverordnung, S. 96 Rn. 394; *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 88 Rn. 20; *Schätzle*, PinG 2017, 203 (205); *Schantz*, NJW 2016, 1841 (1845).

[679] *Kugelmann*, DuD 2016, 566 (567); *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Engeler*, ZD 2018, 55 (58f.); *Schneider*, Datenschutz, S. 164 ff.; *Gola*, K&R 2017, 145 (147); *Selk*, DANA 2016, 59 (61); *Klement,* in: NK Datenschutzrecht Art. 7 Rn. 58.

[680] *Schulz* in: Gola DS-GVO Art. 7 Rn. 26; *Gola*, K&R 2017, 145 (147); *Klement,* in: NK Datenschutzrecht Art. 7 Rn. 62; ähnlich *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 19 f.

[681] *Kugelmann*, DuD 2016, 566 (567); *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 22; *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 42; *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 19. *Engeler* nimmt hingegen eine Prüfpflicht an. Der Regulierungsintention entgegensetzend argumentiert er, dass aus der Regelung zunächst die grundsätzliche Anerkennung der Überschreitbarkeit der Erforderlichkeitsgrenze durch eine Einwilligung folge: *Engeler*, ZD 2018, 55 (59).

[682] *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 38.

[683] Eine starke Position sei anzunehmen, wenn der Verantwortliche die Vertragserfüllung von der Einwilligungserteilung abhängig machen kann und es dem Betroffenen nicht freisteht, die gewünschte Leistung anderweitig zu erhalten: *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 20.

[684] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 165 Die Grundversorgung sei bei Telefon- und Internetzugang erfüllt. Dagegen zählt *Gola* den Personenverkehr, die Versorgungswirtschaft, das Versicherungswesen und soziale Netzwerke zu Formen von relevanten, monopolartigen Angeboten, die das Kopplungsverbot eröffnen sollten: *Gola*, K&R 2017, 145 (147).

[685] *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Schulz,* in: Gola DS-GVO Art. 7 Rn. 25; *Gola*, K&R 2017, 145 (147).

[686] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 165.

[687] *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 33; *Schulz,* in: *Gola*, Gola DS-GVO Art. 7 Rn. 23; *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (91); *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 21; *Malgieri*, International Review of Law, Computers & Technology 2018, 118 (129); *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 21; *Heckmann/Paschke,* in: Ehmann/Selmayr - DSGVO Art. 7 Rn. 96; *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 51.

Umstritten ist, ob eine auf der Einwilligung beruhende Datenverarbeitung nach Widerruf auf eine andere Legitimationsgrundlage gestützt werden kann.[688] Da dem Grenzen gesetzt sind, sollten von Beginn an Datenverarbeitungen nur dann auf die Einwilligung gestützt werden, wenn eine Verarbeitung nach Widerruf unterbleiben kann. Erfordert die Erfüllung einer vertraglichen Pflicht oder Erbringung einer Dienstleistung eine fortgeführte Verarbeitung dieser Daten, war die Einwilligung offensichtlich nicht die richtige Wahl. Liegt eine andere Rechtsgrundlage vor, sollten zudem keine zusätzlichen Einwilligungen „zur Absicherung" eingeholt werden, um das Instrument der Einwilligung nicht zum rein formalisierten Akt verkommen zu lassen.[689] Werden personenbezogene Daten im Rahmen einer vertraglich geschuldeten Diensterbringung auf Grundlage der Einwilligung erhoben, muss es sich um optionale Daten handeln.

6.1.6 Fazit

Die Einwilligung ist Ausdruck der informationellen Selbstbestimmung – stößt im digitalen Zeitalter allerdings immer mehr an praktische Grenzen und droht zur bloßen Fiktion zu werden. [690] Eine Einschränkung der sozialen, auf digitaler Kommunikation basierenden Anbindung an das lebensnotwendige soziale Umfeld kann erhebliche Zwangswirkungen auslösen, insbesondere wenn weitere Transparenzdefizite im Hinblick auf die Tragweite der Einwilligung hinzukommen. Wie weit die Schutzwirkung der Einwilligung reicht, hängt maßgeblich von der Auslegung der Wirksamkeitsvoraussetzungen, vornehmlich dem Merkmal der Freiwilligkeit, ab. Folgende Faktoren sprechen in der Regel gegen die Wirksamkeit einer Einwilligung:

- Das KI-System kommt im Rahmen einer Leistung zum Einsatz, der eine Monopolstellung beigemessen werden kann oder keine/kaum vergleichbare Wechselalternativen bestehen,
- Netzwerkeffekte führen zu einem Lock-In-Effekt, sodass ein Wechsel auf eine andere Leistung zwar theoretisch möglich, aber faktisch ausgeschlossen ist,[691]
- Fälle der Daseinsvorsorge: Insofern wird diskutiert, ob eine „soziale Grundversorgung" bei Kommunikationsformaten oder sozialen Medien anzunehmen ist, ohne deren Zugang eine kommunikative Ausgrenzung zu befürchten wäre.[692]

Art. 7 Abs. 4 DS-GVO steht einer Einwilligung hingegen dann nicht entgegen, wenn zumutbare, alternative Zugangsmöglichkeiten ohne Einwilligungserfordernis zur Verfügung stehen.[693] Dies wäre der Fall, wenn ein

[688] Siehe Abschnitt 2.4.6.1.1.
[689] Zur Beobachtung einer Art „Klickermüdung": *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 17; vgl. auch die Befürchtung eines „Choice Overload": *Hermstrüwer*, Informationelle Selbstgefährdung, S. 369; *Richter*, PinG 2018, 6 (7). Zu Problemen der Einwilligung: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 310 m.w.N.
[690] *Kamp/Rost*, DuD 2013, 80 (82); *Roßnagel u. a.*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, S. 91; *Seidel*, ZG 2014, 153 (155).
[691] Vgl. hierzu: *Schantz*, NJW 2016, 1841 (1845). *Schwartmann/Hentsch*, RDV 2015, 221 (228); *Kamp/Rost*, DuD 2013, 80 (82); a.A. *Buchner*, DuD 2010, 39 (41).
[692] *Kamp/Rost*, DuD 2013, 80 (82).
[693] *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 33; *Metzger*, AcP 2016, 817 (824); *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 101; *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Heckmann/Paschke,* in: Ehmann/Selmayr - DSGVO Art. 7 Rn. 96; *Schafft/Ruoff*, CR 2006, 499 (504).

gleiches Angebot desselben Anbieters auch ohne Einwilligung bereitgestellt wird – sofern dieses nicht unangemessen teurer ausfällt.[694] Andere wollen auch ein vergleichbares Angebot von Drittanbietern als ausreichend gelten lassen.[695] Hinzu kommt, wenn in einem monopolistisch oder oligopolistisch geprägten Markt mit geringen Ausweichmöglichkeiten der berufliche oder soziale Status tangiert ist.[696] Insofern treffen bei der Nutzung von KI-Systemen im Unternehmen mehrere wesentlich die Freiwilligkeit hemmende Faktoren aufeinander: die durch Gruppendynamik entstehende Abhängigkeit von einer Leistung (Netzwerkeffekte, Lock-In), die Bedeutung für die Teilhabe an digitalen Kommunikationsprozessen sowie das Abhängigkeitsverhältnis und die Weisungsgebundenheit im Beschäftigungsverhältnis. Intensiv wurde die Frage eines mittelbar wirkenden Zwangs in Dreieckskonstellationen Arbeitgeber*in – betroffene Person – Verantwortlicher/Dienstanbieter im Rahmen der Corona-Warn-Apps diskutiert.[697] Insofern ist hierbei zu klären, ob externe Effekte dem Verantwortlichen zurechenbar sind.[698] Die Frage ist nicht leicht zu beantworten, ob selbst bei erheblichem externem Druck die gesetzlichen Minimalanforderungen der DSGVO erfüllt sind, oder ob hier eine Einwilligung schlechthin ausscheidet.[699] Insofern könnte zwischen einer dienstlichen Anordnung und einer Empfehlung durch den:die Arbeitgeber*in differenziert werden – wobei auch letztere sozialen Druck ausüben kann.[700]

Als Zwischenergebnis lässt sich folgendes festhalten: Möchte ein Unternehmen die Nutzung eines KI-Systems auf Basis einer Einwilligung gegenüber seinen Beschäftigten eröffnen, anregen oder gar anordnen, bestehen erhebliche Zweifel an der Wirksamkeit einer solchen Einwilligung. Daher ist es zu empfehlen, Angebote zu nutzen, für die keine Erteilung einer Einwilligung erforderlich ist. Unschädlich könnte hingegen die Einräumung der Möglichkeit zur Einwilligung bei reinen Zusatzfunktionalitäten sein.

6.2 Vertrag

Eine Datenverarbeitung ist auch dann rechtmäßig, wenn die Erfüllung eines Vertrags dies erfordert. Wichtig dabei ist, dass die betroffene Person selbst die Vertragspartei sein muss. Die Verarbeitung selbst kann hingegen auch von einem Dritten durchgeführt werden, sofern dies für die Erfüllung des Vertrags mit der betroffenen Person erforderlich ist.[701] Dies gilt auch unabhängig von der Vertragsart.[702] Entscheidend sind somit:

- Das Merkmal der Erforderlichkeit.
- Die Qualifikation der betroffenen Person als Vertragspartei

> **Art. 6 Abs. 1 Buchst. b DSGVO** die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person

[694] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 9; *Gierschmann*, ZD 2016, 51 (54). *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 71 Rn. 44. *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 101.
[695] *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 33; *Brockmeyer*, ZD 2018, 258 (262); *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 19 f. *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 52.
[696] *Metzger*, AcP 2016, 817 (823f.) bezogen auf die privat oder beruflich motivierte Mitgliedschaft in sozialen Netzwerken.
[697] *Samardzic/Becker*, EuZW 2020, 646 (652); *Köllmann*, NZA 2020, 831 (832).
[698] Ablehnend: *Samardzic/Becker*, EuZW 2020, 646 (652).
[699] Vgl. Bedenken bei: *Köllmann*, NZA 2020, 831 (832).
[700] *Köllmann*, NZA 2020, 831 (835).
[701] *Albers/Veit,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 6 Rn. 30; *Schantz,* in: NK Datenschutzrecht Art. 6 Rn. 22; *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 2 Rn. 26.
[702] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 290 f.

erfolgen;

Im Hinblick auf das Vertragsverhältnis zu den Beschäftigten auf Grundlage des Arbeitsvertrags ist § 26 BDSG lex specialis (zu den Anforderungen siehe Abschnitt 8.4.2).[703]

6.2.1 Erforderlichkeit

Eine Datenverarbeitung kann nur über einen Vertrag legitimiert werden, wenn diese zur Vertragserfüllung tatsächlich erforderlich ist. Hier kann eine strenge oder weniger strenge Auslegung vorgenommen werden:

Extensive Auslegung: nach einer Ansicht definiere der jeweilige Dienstanbieter die Leistung in den konkret vorliegenden Vertragsklauseln, sodass sich die Erforderlichkeit stark von den Nutzungsbestimmungen ableite.[704] Kritisiert wird, dass der Vertragspartner dann sein angebotenes Leistungsspektrum beliebig weit formulieren könne und so weitreichende Datenverarbeitungen legitimieren könnte.[705] Anbieter könnten mit dem Angebot zahlreicher Zusatzleistungen ein beliebig weites Gesamtpaket schnüren, unabhängig davon, ob die Nutzenden dieses tatsächlich auch abrufen wollen.

Restriktive Auslegung: Nach einer restriktiven Auslegung des Erforderlichkeitsbegriffs ist dieses Tatbestandsmerkmal nur gegeben, wenn der Leistungserfolg einer Primär- oder Sekundärpflicht ohne die Datenverarbeitung nicht herbeigeführt werden kann, d.h. Unmöglichkeit i.S.d. § 275 Abs. 1 BGB ohne Durchführung der Datenverarbeitung gegeben wäre.[706] Demnach wäre eine objektiv-abstrakte Bestimmung des funktionalen Vertragsgegenstands zu Grunde zu legen.[707] Diese könnte sich am für den jeweiligen Vertragstypus aufgrund hergebrachter wirtschaftlicher Erfahrungen allgemein anzunehmenden Wesenskern bzw. eigentlichen Sinn der vertraglichen Austauschbeziehung orientieren.[708] Bezieht sich der KI-basierte Verarbeitungsvorgang nicht auf den Kern bzw. Hauptgegenstand des Vertrags, kann die Verarbeitung nicht auf diese Rechtsgrundlage gestützt werden.[709]

Beanstandet wird an dieser abstrakt-wertenden Herangehensweise wiederum die Gefahr der Unbestimmtheit, insbesondere bei komplexeren Vertragskonstellationen, sowie mögliche Übertragungsschwierigkeiten der hergebrachten Erfahrungssätze auf moderne, unkonventionelle Vertragsgestaltungen.[710] Befürchtet wird

[703] *Wolff/Kosmider*, ZD 2021, 13 (14); *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 20; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 7.

[704] *Żdanowiecki*, DSRITB 2018, 559 (566); *Malgieri*, International Review of Law, Computers & Technology 2018, 118 (129); *Engeler*, ZD 2018, 55 (57). *Schantz* stellt entscheidend auf die Erkennbarkeit ab, da nur dann die Vereinbarung vom Willen der Parteien getragen wird: *Schantz,* in: NK Datenschutzrecht Art. 6 Rn. 25 ff.

[705] *Graf von Westphalen/Wendehorst*, BB 2016, 2179 (2179). *Radlanski* bezeichnet dies als „konstruierte Erforderlichkeit". Eine weitere Möglichkeit, die Erforderlichkeit auszudehnen, liegt in der tatsächlichen Erweiterung des Funktionsumfangs: *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 119.

[706] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 8; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 21; *Albers/Veit,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 6 Rn. 32; *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 20; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 6 Rn. 11; *Golland*, MMR 2018, 130 (130); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (220).

[707] vgl. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 43 f.; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 22.

[708] *Buchner/Petri,* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 39 ff.

[709] *Niemann/Kevekordes*, CR 2020, 17 (23).

[710] *Engeler*, ZD 2018, 55 (57); a.A. *Härting*, CR 2016, 735 (740) weist darauf hin, dass sich auch im Bereich der digitalen Inhalte Geschäftsmodelle etabliert haben, die Nutzererwartungen prägen.

außerdem eine Hemmungswirkung für Vertragsgestaltungsentwicklungen.[711] Sofern mit der extensiven Auslegung dagegen das Kriterium der Erforderlichkeit durch die bewusste Ausformung des konkreten Vertragsinhalts grundsätzlich frei und privatautonom gesteuert werden kann, verschiebt sich die Prüfung der Wirksamkeit von einer datenschutzrechtlichen Kontrolle auf die Wirksamkeitskontrolle nach §§ 134, 138, 242 BGB bzw. § 305 ff. BGB, wenn es sich um allgemeine Geschäftsbedingungen handelt.[712] In letzterem Fall umfasst die AGB-Kontrolle jedoch nicht die Leistungsbestimmung selbst.[713] Weitere Argumente streiten für die restriktive Auslegung:

- **Einheitliche Auslegung:** Im Rahmen des Art. 6 Abs. 1 DSGVO findet sich die Anforderung der Erforderlichkeit mehrfach. Im Zusammenhang mit primär öffentlich-rechtlich motivierter Datenverarbeitung wird die „Erforderlichkeit" im Sinne einer zwingenden Voraussetzung verstanden, d.h. dass das jeweils angestrebte Ziel ohne Datenverarbeitung anders nicht erreicht werden kann.[714] Dagegen befürworten Einzelstimmen unterschiedliche Maßstäbe für Datenverarbeitung durch staatliche Stellen gegenüber denen durch den Privatrechtsverkehr.[715] Zwar sind private Stellen anders als staatliche nicht direkt Grundrechtsverpflichtete.[716] Den Staat treffen jedoch im Rahmen der mittelbaren Drittwirkung der Grundrechte Handlungspflichten ein angemessenes Schutzniveau sicherzustellen.[717]
- **Abgrenzung zur Einwilligung:** Während sich im Zivilrecht der auf der Privatautonomie basierende Gestaltungswille der Parteien im Vertrag manifestiert, ist die Einwilligung das Steuerungsinstrument für autonome Entscheidungen im Datenschutzrecht.[718] Insofern bestehen auch besondere Aufklärungs- und Transparenzpflichten sowie Widerrufsrechte (vgl. Art. 7 DSGVO), welche durch eine extensive Auslegung des Art. 6 Abs. 1 Buchst. b DSGVO nicht umgangen werden sollten.[719]
- **Orientierung am Grundsatz der Datenminimierung**: Bereits im Rahmen der Datenschutzrichtlinie bestand Streit darüber, ob Erforderlichkeit eng mit „Unerlässlichkeit" oder weiter mit der „vernünftigerweise" zur Sicherung der ordnungsgemäßen Vertrags- bzw. Nutzungsdurchführung gleichzusetzen war.[720] Soweit die Erforderlichkeit beliebig steuerbar ist, drohen allerdings Ziele wie die Datenminimierung sowie deren Konkretisierung im Rahmen des *Privacy by Design* und *Privacy by Default* gemäß Art. 25 DS-GVO unterlaufen zu werden.[721]

Erste Gerichtsurteile scheinen eine vermittelnde Position einzunehmen, wonach zwar kein strenger Maßstab

[711] *Engeler*, ZD 2018, 55 (57).
[712] Die Prüfung der Treuwidrigkeit und der guten Sitten würde dem „ansonsten der Beliebigkeit anheimfallenden Erforderlichkeitsbegriff die nötige Bestimmtheit verleihen": *Engeler*, ZD 2018, 55 (57, 60).
[713] BGH, Urteil vom 05. Oktober 2017 – III ZR 56/17 –, Rn. 15; BGH, Urteil vom 22. September 2016 – III ZR 264/15 –, Rn. 12; BGH, Urteil vom 09. Oktober 2014 – III ZR 32/14 –, Rn. 37; BGH, Urteil vom 13. Januar 2011 – III ZR 78/10 –, Rn. 15; BGH, Versäumnisurteil vom 06. Juli 2011 – VIII ZR 293/10 –, Rn. 10; BGH, Urteil vom 12. Juni 2001 – XI ZR 274/00 –, BGHZ 148, 74-84, Rn. 12; BGH, Urteil vom 12. Dezember 2000 – XI ZR 138/00 –, BGHZ 146, 138-144, Rn. 12; BGH, Urteil vom 24. März 1999 – IV ZR 90/98 –, BGHZ 141, 137-152, Rn. 25; kritisch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749).
[714] *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 28 ff. *Buchner/Petri,* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 15.
[715] *Frenzel,* in: Paal/Pauly, DS-GVO Art. 6 Rn. 14.
[716] *Frenzel,* in: Paal/Pauly, DS-GVO Art. 6 Rn. 14.
[717] Siehe Abschnitt 2.1.3.3.
[718] vgl. *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 29; *Stemmer,* in: BeckOK DatenschutzR Art. 7 Rn. 41; *Nebel*, K&R 2019, 148 (150); *Buchner/Petri,* in: Kühling/Buchner - DS-GVO/BDSG Art. 6 Rn. 26; *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 18.
[719] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 299; *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747); *Buchner/Petri,* in: Kühling/Buchner - DS-GVO/BDSG Art. 6 Rn. 26.
[720] BT-Drs 13 / 7385, S. 24; *Müller-Broich*, TMG, § 14 Rn. 3; *Spindler/Schuster*, Recht der elektronischen Medien, § 14 TMG Rn. 4. *Plath*, BDSG, § 14 TMG Rn. 13.; vgl. auch BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69, Rn. 30 ff.
[721] *Engeler*, ZD 2018, 55 (57).

anzulegen sei, d.h. nicht erst bei Unmöglichkeit von der Erforderlichkeit auszugehen sei, die Kriterien nichtsdestotrotz *objektiv* zu bestimmen sind.[722] Die Verarbeitung muss nach vernünftiger Würdigung objektiv sinnvoll im Kontext des Vertragszwecks sein.[723] Erforderlichkeit ist bei den *essentialia negotii* (lateinisch für wesentliche Geschäftseigenschaften)[724] des Vertrags gegeben.[725]

6.2.2 Vertrag mit der betroffenen Peron

Nach dem Wortlaut der DSGVO kommt Art. 6 Abs. 1 Buchst. b) DSGVO nur in Betracht, wenn die betroffene Person selbst Vertragspartei ist bzw. vorvertragliche Maßnahmen auf ihre Anfrage erfolgen. Nun sind Konstellationen denkbar, in denen eine Datenverarbeitung für die Durchführung eines Vertrages erforderlich sind, aber auch Daten Dritter erfassen.

Beispiele:

Mobilitätsdienstleistung: Ein Unternehmen bietet ein autonomes On-Demand-Shuttle an. Da dieses fahrerlos fährt, muss eine Technische Aufsicht über eine Leitzentrale das Fahrzeug betreuen, um im Notfall eingreifen zu können. Die Zulassungsbehörde verlangt hierfür den Einbau von Videokameras. Ein automatisches Sturzdetektionssystem soll zudem im Innenraum sicherstellen, dass bei Gefahrensituationen ein Not-Stopp durchgeführt wird. Zu Abrechnungszwecken werden zudem Identifikationsdaten des:der jeweiligen Kund*in erhoben und verarbeitet. Kunde M nutzt das Shuttle regelmäßig mit seiner gesamten Familie.

Unternehmen als Vertragspartner: Unternehmen A unterhält Vertragsbeziehungen zu Unternehmen B. Vertragsparteien sind somit die juristischen Personen, vertreten durch den jeweiligen Vorstand. Im Rahmen der Erfüllung der vertraglichen Verpflichtungen kommunizieren Mitarbeiter miteinander über einen Messengerdienst. Unternehmen A möchte diese Kommunikation zu Beweis- und Abrechnungszwecken aufzeichnen.

In Teilen der Literatur wird zur Lösung solcher Fälle ein weites Verständnis der „Vertragspartei“ präferiert.[726] Die überwiegende Ansicht in Literatur und Rechtsprechung scheint dieser Interpretation allerdings bisher nicht zugetan und verweist auf den eindeutigen Wortlaut.[727] Die Norm macht hingegen keine Angaben, wer auf Seiten des Verantwortlichen Vertragspartei sein muss: grundsätzlich kann auch die Verarbeitung durch einen Dritten legitimiert werden, wenn dies zur Vertragserfüllung erforderlich ist. [728] Somit lassen sich mehrere Lösungsoptionen diskutieren:

A. weite Interpretation des „Vertrags“ und Einbeziehung Dritter, wie bspw. bei Verträgen mit Schutzwirkung zugunsten Dritter,
B. Betrachtung von Vertragsketten zwischen unterschiedlichen Personen, oder
C. Kombination mehrerer Rechtsgrundlagen.

Im ersten Beispiel könnte der Einsatz der Videokameras und des Sturzdetektionssystems gegenüber den Familienmitgliedern, die nicht selbst Vertragspartei sind, auf eine Interessenabwägung gestützt werden. Das

[722] VG Mainz, Urteil vom 20.2.2020 – 1 K 467/19.MZ, Rn. 30.
[723] OLG München, Urteil vom 16.1.2019 – 7 U 342/18, Rn. 30
[724] Essentialia negotii bezeichnen die wesentlichen Vertragsbestandteile, ohne die kein sinnvoller Vertrag zustande käme.
[725] VG Mainz, Urteil vom 20.2.2020 – 1 K 467/19.MZ, Rn. 30; kritisch: *Blasek*, ZD 2020, 376 (379).
[726] Für die Einbeziehung Daten Dritter: *Taeger,* in: Taeger/Gabel - DSGVO/BDSG Art. 6 Rn. 61.
[727] *Wolff/Kosmider*, ZD 2021, 13 (14); *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 6 Rn. 13; *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 30; *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 28; *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 18.; vgl. auch OLG München, Urteil vom 16.1.2019 – 7 U 342/18, Rn. 30; VG Mainz, Urteil vom 20.2.2020 – 1 K 467/19.MZ, Rn. 29.
[728] *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 30.

Unternehmen kann ein berechtigtes Interesse an einer möglichst verkehrssicheren Bereitstellung von autonomen Shuttles geltend machen und müsste dem die berechtigten Erwartungen der betroffenen Personen gegenüberstellen: hier dürfte auch der Faktor eine Rolle spielen, dass die Nutzung des Shuttles durch die Familie bewusst erfolgt, sofern die Datenverarbeitung transparent und erkennbar ist.

Im Beschäftigungskontext liegt ein Vertrag der Beschäftigten mit ihren Arbeitgebern in Form des Arbeitsvertrags vor – dabei kommt es aber zu einer lex specialis-Anwendung des § 26 BDSG: für eine Rechtfertigung müssten die Datenverarbeitungen durch Geschäftskontakte zur Durchführung des Beschäftigungsverhältnisses erforderlich sein.[729] Dies betrifft die Offenlegung durch das Vertragspartnerunternehmen in seiner Funktion als Verantwortlicher gegenüber dem den Messengerdienst bereitstellenden Unternehmen – ob es auch den gesamten Kommunikationsprozess als einheitlichen Lebenssachverhalt erfasst, ist allerdings mit einigen Unsicherheiten behaftet. [730] Im Endeffekt verbleibt es bei einem Rekurs auf die Interessenabwägung.[731] Bei Videokonferenzen können laut DSK berechtigte Interessen die Datenverarbeitung legitimieren, wenn grundsätzlich Alternativen zur Videokonferenz verbleiben und die Beschäftigten anderer Unternehmen teilnehmen.[732] Organisatorisch müssen Verantwortliche beachten, dass betroffenen Personen ein Widerspruchsrecht nach Art. 21 DSGVO zusteht, wenn die Verarbeitung auf der Interessenabwägung beruht.

6.2.3 Zwischenergebnis zum Vertrag

Bei strenger Auslegung des Kriteriums der Erforderlichkeit, kann diese Rechtsgrundlage nur die zwingend *notwendigen*, personenbezogenen Daten erfassen. Für Daten, welche lediglich *nützlich* sind, bspw. um die User-Experience zu steigern, wäre fraglich, ob dies den Vertragserfolg tangiert. Wird diese Datenbereitstellung optional gestaltet, wäre wiederum eine Einwilligung denkbar. Diese darf allerdings nicht an die Vertragserfüllung gekoppelt werden (insbesondere, wenn weitere die Freiwilligkeit ausschließende Merkmale hinzukommen), sondern es sollte dann auch möglich sein, das System ohne die entsprechende Datenbereitstellung zu nutzen. Kommt es beim Einsatz des KI-Systems zur Verarbeitung der personenbezogenen Daten Dritter, lassen sich regelmäßig Lösungen über die Kombination mehrerer Rechtsgrundlagen finden. Diskutiert wird daneben über ein weites Verständnis.

6.3 Lebenswichtige Interessen

In Notlagen muss der Datenschutz gegenüber dem Schutz lebenswichtiger Interessen zurücktreten: nach ErwGr. 112 S. 2 sind darunter insbesondere die körperliche Unversehrtheit und das Leben umfasst.[733] Dabei sollte nach ErwGr. 46 S. 2 der Schutz eines lebenswichtigen Interesses nur dann eingreifen, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Somit hat die Regelung subsidiären Charakter.[734]

[729] *Wolff/Kosmider*, ZD 2021, 13 (14 f.); vgl. auch *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 91 ff.; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 39.
[730] *Wolff/Kosmider*, ZD 2021, 13 (14 f.).
[731] *Wolff/Kosmider*, ZD 2021, 13 (16).
[732] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 10.
[733] *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 51.
[734] *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 51.

> **Art. 6 Abs. 1 Buchst. d DSGVO** die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen

ErwGr. 46 nennt Beispiele, in denen sowohl wichtige Gründe des öffentlichen Interesses als auch lebenswichtige Interessen tangiert sein können: humanitäre Zwecke, Überwachung von Epidemien, humanitäre Notfälle, wie Naturkatastrophen oder vom Menschen verursachte Katastrophen. In vielen dieser Fälle werden sich Spezialregelungen im Rahmen der Beschreibung öffentlicher Aufgaben finden. Die Relevanz der Norm zeigt sich somit vor allem bei akuten Notsituationen.[735]

6.4 Interessenabwägung

> **Art. 6 Abs. 1 Buchst. f DSGVO** die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Im Rahmen des Art. 6 Abs. 1 Buchst. f DSGVO ist das berechtigte Interesse des Verantwortlichen oder eines Dritten an der Verarbeitung der personenbezogenen Daten mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Peron(en) in Relation zu setzen.[736] Grundsätzlich handelt es sich um eine Einzelfallabwägung – selbst im Fall von Konsequenzen für eine Vielzahl von Personen.[737] Insofern sind drei wesentliche tatbestandsmerkmale zu prüfen:

- Berechtigtes Interesse des Verantwortlichen / eines Dritten
- Erforderlichkeit
- Überwiegen der Interessen

6.4.1 Berechtigtes Interesse

Jedes rechtmäßige rechtliche, tatsächliche, wirtschaftliche oder immaterielle Interesse.[738]Anhaltspunkte für berechtigte Interessen finden sich in den ErwGr. 47, 48 und 49.

Beispiele in den ErwGr. 47, 48, 49 DSGVO:

- IT-Sicherheit
- Betrugsprävention[739]
- Konzerndaten (Übermittlung innerhalb von Unternehmensgruppen)
- Direktwerbung

[735] *Köllmann*, NZA 2020, 831 (833).
[736] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 6 Rn. 14; *Wolff/Kosmider*, ZD 2021, 13 (16).
[737] *Schefzig*, DSRITB 2018, 491 (495).
[738] *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 30 ff.; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 6 Rn. 22.
[739] Zweifelnd, ob beschränkbar auf das *„unbedingt erforderliche“* Maß, im Hinblick auf umfangreiche KI-basierte Analysen: *Gausling*, DSRITB 2018, 519 (531).

6.4.2 Erforderlichkeit

Erforderlichkeit ist nicht gegeben, wenn ein milderes, gleich effizientes Mittel vorhanden ist.[740] Existieren datenschutzfreundliche Lösungen, deren Einsatz technisch möglich und wirtschaftlich zumutbar ist, ohne die Verarbeitungsziele zu beeinträchtigen, lässt sich eine Verarbeitung ohne Einsatz dieser Lösungen nur schwer begründen.[741] Eine Datenverarbeitung kann Erforderlich sein, wenn Alternativen technisch und organisatorisch nicht oder nur mit einem unzumutbaren wirtschaftlichen Aufwand umsetzbar sind, bspw. wenn datenschutzfreundliche Technik nicht am Markt verfügbar ist.[742]

6.4.3 Überwiegen der Interessen

Bei der Abwägung können die unterschiedlichen Grundrechte, wie bspw. Informations-, Presse- und Meinungsfreiheit oder die Berufsausübung eine Rolle spielen.[743] ErwGr. 47 DSGVO benennt zudem die potentiellen Folgen und vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zum Verantwortlichen beruhen. Dabei soll nach Ansicht des EDSA nicht ausschließlich auf die subjektiven Erwartungen der konkret betroffenen Personen, sondern vielmehr an den Erwartungen eines objektiven Dritten in der konkreten Situation abgestellt werden.[744] Weitere Abwägungskriterien sind: Intensität, u. a. durch die Art der gesammelten Informationen (Informationsgehalt), Umfang (Informationsdichte), Anzahl der betroffenen Personen, tatsächlichen Interessen der Gruppe der betroffenen Personen, Verfügbarkeit alternativer Mittel sowie Art und Umfang der Datenbewertung.[745]

Problematisch erscheinen Systeme, bei denen die konkrete Entscheidungsfindung nicht prädeterminiert ist, d.h. die zum Zeitpunkt der Programmierung nicht erkennbar ist, welche Konsequenzen er Einsatz für betroffene Personen haben könnte. [746] *Schefzig* schlägt vor, entsprechende Grundregeln zu programmieren, die einen festen Rahmen vorgeben. [747]

Weitere Praxistipps bestehen in der Implementierung privatsphärenschützender Maßnahmen, um die Abwägung zugunsten der berechtigten Interessen zu beeinflussen:

- *Anonymisierung:* Ist der Personenbezug im jeweiligen Kontext nicht erforderlich, wäre in diesem Fall nur noch der Vorgang der Anonymisierung selbst als Verarbeitung zu rechtfertigen.[748] Da die Anonymisierung gerade dem Betroffenenschutz dient, sprechen gute Argumente für eine Rechtfertigung. [749] Selbst die Anwendung von Anonymisierungsmethoden, die keine Anonymität im Rechtssinne erreichen, kann durchaus geeignet sein die Eingriffsintensität einer Datenverarbeitung abzusenken.[750]
- *Pseudonymisierung:* Sofern eine Anonymisierung nicht möglich ist, wäre an eine Pseudonymisierung

[740] *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 37.
[741] Vgl. BGH, Urteil vom 15. Mai 2018, VI ZR 233/17, Rn. 25 (noch zur alten Rechtslage im Hinblick auf das Merkmal der Erforderlichkeit).
[742] Vgl. OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, CR 2017, 805 (807).
[743] *Albers/veit,* in: BeckOK DatenschutzR Art. 6 Rn. 49.
[744] *European Data Protection Board*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Angenommen am 29. Januar 2020, S. 13.
[745] *European Data Protection Board*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Angenommen am 29. Januar 2020, S. 12.
[746] *Schefzig*, DSRITB 2018, 491 (495).
[747] *Schefzig*, DSRITB 2018, 491 (495 ff.).
[748] *Niemann/Kevekordes*, CR 2020, 17 (23).
[749] *Niemann/Kevekordes*, CR 2020, 17 (23).
[750] *Balaban/Wagner*, Minimizing the Risks of Data Protection Infringement - Data Lifecycle Risk Assessment.

zu denken, um Betroffeneninteressen zu schützen.

- *Datenauswahl:* Sicherstellung hoher Relevanz und Repräsentativität der Daten mit möglichst geringer Fehlerrate des Algorithmus sowie heterogene Auswahl um Diskriminierung vorzubeugen.[751]
- *Graduelle Intensität:* Gegenüber unüberwachtem Lernen verspricht überwachtes Lernen mehr Kontrolle und die bessere Umsetzung der Transparenz- und Betroffenenrechte.[752] Die Entscheidungsweise nicht-deterministischer Systeme birgt gegenüber deterministischen (d. h. vollständig vorhersehbare) aufgrund der limitierten Vorhersehbarkeit risikobehafteter für unvorhergesehene Fehlentscheidungen – insbesondere bei im Betrieb weiterlernenden Systemen.[753]
- *Robustheit* gegenüber Manipulationen.[754]

6.4.4 Widerspruchsrecht

Gegenüber Datenverarbeitungen, die auf eine Interessenabwägung gestützt werden, gewährt Art. 21 DSGVO das Recht, der Datenverarbeitung im Einzelfall zu widersprechen.

Verarbeitung auf Grundlage von Art. 6 Abs. 1 Buchst. e oder f DSGVO	Verarbeitungen für Zwecke der Direktwerbung	Verarbeitung zu Forschungszwecken oder statistischen Zwecken
Voraussetzung: Angabe von Gründen, die sich aus ihrer besonderen Situation ergeben	Keine zusätzlichen Voraussetzungen	Voraussetzung: Angabe von Gründen, die sich aus ihrer besonderen Situation ergeben
Folge: Unterlassen der Verarbeitung personenbezogener Daten, es sei denn: – Nachweis zwingender schutzwürdiger Gründe, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder – Verarbeitung dient Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen	Folge: Unterlassen der Verarbeitung personenbezogener Daten zu diesen Zwecken	Folge: Unterlassen der Verarbeitung personenbezogener Daten, es sei denn: – Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich

Besondere Gründe, die von der in der Interessenabwägung zugrunde gelegten Ausgangslage wesentlich abweichen, sind bspw. Gefahren für Leib und Leben, das Eigentum oder für in ihrer Bedeutung vergleichbare (absolute) Rechtspositionen oder Konstellationen, die ethische, soziale, gesellschaftliche oder familiäre

[751] *Niemann/Kevekordes*, CR 2020, 17 (23); vgl. hierzu die Empfehlungen: *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 7 f.
[752] *Niemann/Kevekordes*, CR 2020, 17 (23); vgl. auch *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 4.
[753] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 6.
[754] *Niemann/Kevekordes*, CR 2020, 17 (24); *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 11.

Zwangssituationen herbeiführen können.[755] Bezüglich der Forschung hat der Gesetzgeber von der Möglichkeit Gebrauch gemacht, das Widerspruchsrecht im Rahmen der Forschungsklauseln einzuschränken (siehe Abschnitt 9.3.4).

6.4.5 Zwischenfazit

Eine durchgeführte Abwägung sollte stets gut dokumentiert werden, um die Erwägungen bei Bedarf einer Aufsichtsbehörde gegenüber belegen zu können.[756] Bezüglich der Verarbeitung personenbezogener Daten der Beschäftigten wird die Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO von § 26 BDSG verdrängt (siehe Abschnitt 8.4.2).[757]

6.5 Erfüllung einer rechtlichen Verpflichtung

Gemäß Art. 6 Abs. 2 DSGVO können die Mitgliedstaaten *spezifische Bestimmungen* zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung zur Erfüllung von Abs. 1 S. 1 Buchst. c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präzise bestimmen, um eine rechtmäßige und nach Treu und Glaube erfolgende Verarbeitung zu gewährleisten.

> **Art. 6 Abs. 1 Buchst. c DSGVO** die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt

Nach Buchstabe c kann mit einer rechtlichen Verpflichtung auch eine Legitimationsgrundlage zur Datenverarbeitung einhergehen. Diese rechtliche Verpflichtung kann sich aus EU-Recht oder aus dem Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, ergeben (Art. 6 Abs. 3 S. 1 DSGVO). Nach dem deutschen Recht könnten beispielsweise folgende rechtliche Verpflichtungen in Betracht kommen:

- Aufzeichnungspflichten (z. B. Fahrtenschreiber, § 57a StVZO) und Dokumentationspflichten (z. B. Arbeitszeitenaufzeichnung nach § 17 Abs. 1 MiLoG),
- Übermittlungspflichten (z.B. beim autonomen / automatisierten Fahren: § 1g, § 63a Abs. 3 StVG),
- Aufbewahrungs- und Speicherpflichten (z. B. § 257 HGB; § 147 AO),
- Pflichten zur Verarbeitung von Kundendaten (z. B. § 312f Abs. 1 BGB),
- Risikominimierungspflichten (vgl. § 10 Abs. 2 KWG),
- Meldepflichten (§ 28a SGB IV),
- Abgleichpflichten (VO (EG) Nr. 881/2002, VO (EG) Nr. 2580/2001, sog. Anti-Terror-Listen), etc.[758]

Beispiel Geschäftskorrespondenz:

Zunächst verpflichten unterschiedliche handels- oder gesellschaftsrechtliche Vorgaben (bspw. § 35a Abs. 1 S. 1 GmbHG, § 80 Abs. 1 AktG, § 37a HGB oder § 125a HGB) im Rahmen der Geschäftskorrespondenz zur Angabe bestimmter Informationen wie Firma, Rechtsform, Sitz des Unternehmens, Post-/Lieferanschrift, Name

[755] *Niemann/Kevekordes*, CR 2020, 179 (181).
[756] *Rohrlich*, ZAP 2020, 1265 (1267).
[757] Vgl. *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 10.
[758] *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 44.

der Ansprechperson und ggf. deren Funktion und / oder Abteilungszugehörigkeit.[759] Im Rahmen der Unternehmenskommunikation könnten daneben insbesondere die gesetzliche Aufbewahrungspflicht nach § 257 HGB und die steuerliche Aufbewahrungspflicht nach § 147 AO für das Unternehmen relevant werden. [760]

6.6 Erfüllung einer Aufgabe im öffentlichen Interesse

> **Art. 6 Abs. 1 Buchst. e DSGVO** die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

Art. 6 Abs. 1 Buchst. e DSGVO betrifft die Datenverarbeitung im öffentlichen Interesse. Adressat sind daher lediglich Stellen, die öffentliche Aufgaben oder im öffentlichen Interesse liegende Aufgaben wahrnehmen.

6.7 Zwischenergebnis

Für jede Verarbeitung personenbezogener Daten muss der Verantwortliche in der Lage sein, eine Rechtsgrundlage vorzuweisen. Dabei können auch mehrere Rechtsgrundlagen parallel eingreifen.

[759] *Helfrich,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 3 B. II. Rn. 14.
[760] *Schrey u. a.*, MMR 2017, 656 (659).

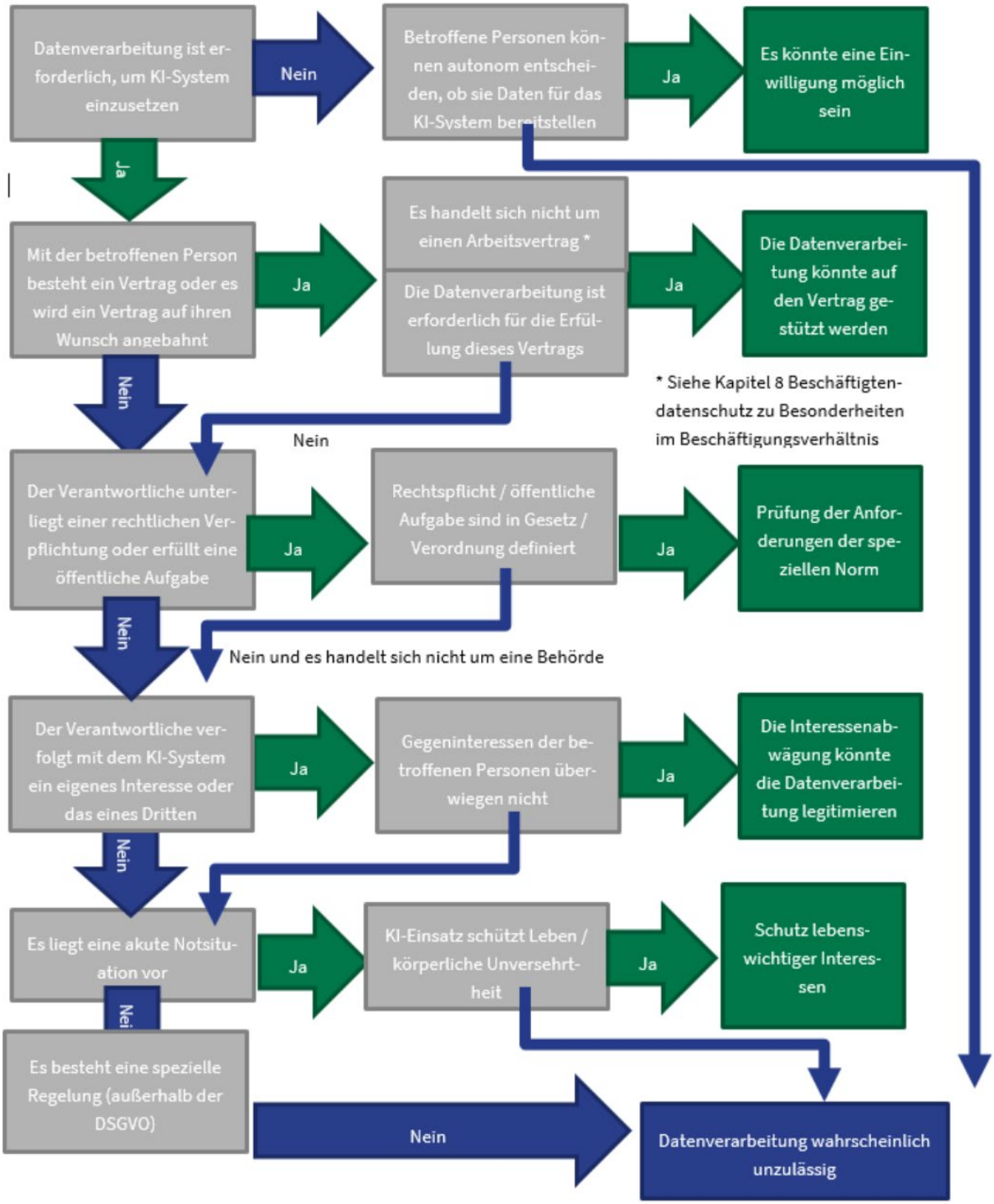


Abbildung 18 Prüfschema zur Auswahl der Rechtsgrundlage

7 KI-Entscheidungen und Datenschutz

Erste Ansätze zur Regulierung der Automatisierung im Zeitalter der künstlichen Intelligenz beinhaltet die DSGVO mit dem Recht keiner ausschließlich automatisierten Entscheidung im Einzelfall einschließlich Profiling unterworfen zu werden (Art. 22 DSGVO). Diese Regelung wird im Folgenden dargestellt und im Hinblick auf Schutzziele, Rollen und Schutzmechanismen mit dem aktuellen EU-Kommissionsentwurf einer KI-Verordnung verglichen.

7.1 Verbot automatisierter Entscheidungen im Einzelfall

Einige Negativbeispiele wie Fehlklassifizierungen von People of Colour, diskriminierende, Ungleichbehandlungen und Vorurteile zementierende Systeme, das Erlernen rassistischen Verhaltens von Chat-Bots oder fehlende Kompetenzen im Umgang mit Kindern zeigen die Beschränkungen und Gefahren heutiger KI-Systeme.[761] Als wesentliche Herausforderungen des Einsatzes von Machine-Learning-Modellen lassen sich zusammenfassen:[762]

- **Abhängigkeit von Trainingsdaten:** Sind Daten statistisch nicht repräsentativ, sind „Verzerrungen“ möglich; historische Daten enthalten oft Benachteiligungen bestimmter Gruppen aufgrund von alten Vorurteilen und Stereotypen.
- **Probabilistischer Charakter:** Ergebnisse sind aufgrund qualitativer Unsicherheiten des Modells, der Eingabe- und Lerndaten nur approximativ. Das System gibt die besten Alternativen aus und könnte diese mit einer Unsicherheitsangabe versehen, um dem Menschen bei der Interpretation zu unterstützen – sofern es nicht vollautomatisch agiert.
- **Verständlichkeit und Transparenz:** Aufgrund der Komplexität ist nur das äußere Verhalten sichtbar, die inneren Funktionsmechanismen aber unzugänglich („Black Box“). Damit ist es oftmals unmöglich das Zustandekommen einer Entscheidung nachzuvollziehen. Forschung zu Explainable AI widmet sich dieser Problematik. „Erklärmodelle“ könnten ermitteln, welche Teile einer Eingabe ausschlaggebend waren.
- **Testen:** Statt des modularen Testens tritt das quantitative Testen des Modells anhand von separaten Testdaten. Lassen sich Modelle nicht in separat prüfbare Einheiten zerlegen, scheitern klassische Softwaretestmethoden.
- **Selbstlernen im Betrieb:** Wird Nutzerfeedback zum automatischen Weiterlernen genutzt, unterliegen Modelle kontinuierlichen Veränderungen. Herausforderungen bestehen darin einen kontrollierten Einsatz durch die Konstruktion von „Leitplanken“ zu etablieren.

Einige dieser Herausforderungen lassen sich derzeit in der Praxis nur über eine engmaschige Überwachung der KI-Anwendung und des entsprechenden Kompetenzaufbaus der Anwender*innen begegnen. [763]

[761] Zu den Beispielen siehe: *Fraunhofer-Allianz Big Data*, Zukunftsmarkt Künstliche Intelligenz - Potenziale und Anwendungen, S. 5 m.w.N. *Martini*, JZ 2017, 1017 (1018) m.w.N.
[762] *Fraunhofer IAIS*, Vertrauenswürdiger Einsatz von Künstlicher Intelligenz, S. 11; zu Hintergründen und Ursachen siehe auch: *Käde/Maltzan*, CR 2020, 66 (66 f.).
[763] *Fraunhofer IAIS*, Vertrauenswürdiger Einsatz von Künstlicher Intelligenz, S. 11.

7.1.1 Grundsatz des Art. 22 DSGVO

Entsprechend dem aus der Menschenwürde folgenden Grundgedanke, dass Menschen nicht zum reinen Objekt der Entscheidung einer Softwareanwendung werden sollen, adressiert die DSGVO vollautomatisierte Entscheidungsverfahren mit einem präventiven Verbot – lässt allerdings zahlreiche Durchbrechungen zu.[764] Art. 22 DSGVO schützt betroffene Personen davor, nicht einer ausschließlich automatisierten Entscheidung, welche auf einer Verarbeitung ihrer personenbezogenen Daten beruht, ohne jegliches menschliche Eingreifen unterworfen zu werden. Darunter ist zu verstehen, dass ein lediglich algorithmenbasierter Datenverarbeitungsprozess, ohne Dazwischentreten eines Menschen einzelne, die Person betreffende persönliche Aspekte weder bewerten soll, noch, dass sich daraus rechtliche Wirkungen entfalten sollen oder andere Wirkungen, welche die betroffene Person erheblich beeinträchtigen können.[765] Trotz der Verortung bei den Betroffenenrechten entfaltet die Norm Verbotscharakter, ohne dass betroffene Personen ihre Rechte aktiv geltend machen müssten.[766]

Automatische Entscheidung und Profiling: Die automatisierte Entscheidungsfindung kann sich teilweise mit Profiling überschneiden oder aus diesem resultieren.[767] Insofern fällt nicht jede Form des Profiling unter Art. 22 DSGVO und nicht jede Art der automatischen Entscheidung basiert auf Profiling. Art. 22 DSGVO greift mit seinem Schutzkonzept nur, wenn es sich um eine *ausschließlich* auf automatisierter Verarbeitung beruhenden *Entscheidung* handelt.[768] Sobald eine eigenständige menschliche Entscheidung dazwischentritt, ist die Norm nicht anwendbar.[769] Dies bedeutet für KI-Systeme, dass ein Freigabe-, Bestätigungs- bzw. Ablehnungsmechanismus durch menschliches Zutun implementiert wird.[770] Erhebliche Argumente streiten allerdings dafür, trotz menschlicher Mitwirkungshandlungen im Entscheidungsprozess von einer ausschließlich automatisch ausgeführten Entscheidung auf Grundlage einer automatisierten maschinellen Verarbeitung auszugehen, wenn die Entscheidung inhaltlich de facto der Maschine überlassen bleibt.[771] Ein „menschliches Eingreifen“ bzw. *eigene* Entscheidung des Menschen wird überwiegend erst dann angenommen, wenn eine inhaltliche Überprüfung des automatisiert generierten Entscheidungsvorschlags durch eine natürliche Person erfolgt, die entsprechend auch einen Entscheidungsspielraum hat.[772] Das Merkmal „ausschließlich“ wäre also auch erfüllt, wenn die menschliche Beeinflussungsmöglichkeit so gering ist, dass diese den Kausalzusammenhang zwischen automatisierter Verarbeitung und Entscheidung nicht aufheben kann.[773] Gefordert wird zudem, dass diese Person Kenntnisse über die Datengrundlage hat und über eine entsprechende fachliche Qualifikation verfügt – nicht erforderlich sei hingegen die Kenntnis über Einzelheiten des Programms oder dessen Algorithmus.[774] Bloße Stichprobenkontrollen oder Anpassung der künstlichen neuronalen Netze zur Verbesserung der Entscheidungen dürften ebenfalls keine ausreichende menschliche Intervention darstellen, sondern eher der Wartung des Systems.[775]

---

[764] *Martini*, JZ 2017, 1017 (1019).
[765] *Brecht u. a.*, PinG 2018, 10 (12).
[766] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (278) m.w.N. *Gausling*, DSRITB 2018, 519 (540).
[767] *Artikel-29-Datenschutzgruppe*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), S. 8.
[768] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 25; *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (278).
[769] *von Lewinski,* in: BeckOK DatenschutzR Art. 22 Rn. 21.
[770] *DSK - Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 18.
[771] *Horstmann/Dalmer*, ZD 2022, 260 (261).
[772] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 26; *von Lewinski,* in: BeckOK DatenschutzR Art. 22 Rn. 25; *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 14.; vgl. auch AG Düsseldorf, Urteil vom 18.1.2018 – 22 C 136/17 (noch zur alten Rechtslage).
[773] *Horstmann/Dalmer*, ZD 2022, 260 (261).
[774] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 27; *von Lewinski,* in: BeckOK DatenschutzR Art. 22 Rn. 24.
[775] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (279).

Automatisierte Entscheidungen können sich auf jede Art von Daten stützen, bspw.:

- von der betroffenen Person hierzu bereitgestellter Daten;
- Daten, die über die betreffenden Personen beobachtet wurden;
- abgeleitete Daten wie ein bereits erstelltes Profil der Person.[776]

Im Beschäftigungskontext werden automatisierte Verarbeitungen bspw. beim sog. *E-Recruiting* eingesetzt: erfolgt hier eine automatisierte Vorauswahl im Vorfeld einer Personalbesetzung handelt es sich lediglich um eine Entscheidungshilfe und wird vom Verbot nicht erfasst.[777] Anders ist der Fall zu beurteilen, wenn Bewerber*innen in die weiteren Auswahlüberlegungen von vornherein nicht mehr einbezogen werden und bereits durch das System eine Absage erhalten.[778]

Die DSGVO nennt Profiling als ein Beispiel der automatischen Entscheidung. Somit ist die Regelung anwendbar, sofern drei Elemente gegeben sind:

- automatisierte Verarbeitung
- durchgeführt mit personenbezogenen Daten und
- mit dem Ziele persönliche Aspekte der betroffenen Person zu bewerten.[779]

Auswirkungen der Entscheidung: Art. 22 Abs. 1 DSGVO nennt zwei Alternativen: sofern diese Entscheidung gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Zunächst ist umstritten, ob im ersteren Fall auch eine erhebliche Beeinträchtigung vorliegen müsse, also das Verbot nur bei negativ wirkenden rechtlichen Wirkungen greift, oder ob jede rechtliche Wirkung erfasst ist, unabhängig von ihrer Einstufung als positiv (begünstigend) oder negativ (beeinträchtigend).[780] Die aktuell im Schrifttum vorherrschende Meinung, scheint eher zu letzterem zu tendieren.[781] ErwGr. 71 führt dazu exemplarisch die Beispiele der Ablehnung eines Online-Kreditvertrages oder Online-Einstellungsverfahrens auf. Fraglich ist auch, ob bspw. die Verweigerung eines Vertragsschlusses unter „rechtliche Wirkung" oder eine „erhebliche Beeinträchtigung" fällt, da eine Änderung des rechtlichen Status gerade ausbleibt und sich für den Grad der Erheblichkeit einer Beeinträchtigung noch keine allgemeine Definition herausgebildet hat.[782]

Beispiele (ErwGr. 71 DSGVO)

- automatische Ablehnung eines Online-Kreditantrags
- automatische Ablehnung eines Online-Einstellungsverfahren

Ausnahmen vom Verbot: Der Ausschluss der Verarbeitung soll nach Absatz 2 nicht gelten, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

[776] *Artikel-29-Datenschutzgruppe*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), S. 8.
[777] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 28; *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 13.; *Frank/Heine*, NZA 2021, 1448 (1452).
[778] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 28; *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 14.
[779] *Artikel-29-Datenschutzgruppe*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), S. 6.
[780] *Brecht u. a.*, PinG 2018, 10 (13); *von Lewsinski,* in: BeckOK DatenschutzR Art. 22 Rn. 33.
[781] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 32; *Helfrich,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 22 Rn. 48; *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 22 Rn. 26; *Hladjk,* in: Ehmann/Selmayr - DSGVO Art. 22 Rn. 9; a.A. sofern einem Begehren vollumfänglich stattgegeben wird: *Buchner,* in: Kühling/Buchner - DS-GVO/BDSG Art. 22 Rn. 25; *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 22 ff. *Taeger,* in: Taeger/Gabel - DSGVO/BDSG Art. 22 Rn. 47.
[782] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (280).

- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.[783]

Art. 22 DSGVO stellt keinen eigenen Erlaubnistatbestand dar, sondern eine zusätzliche Einschränkung im Hinblick auf die Rechtsmäßigkeit.[784]

Schutzmaßnahmen: In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf

- direktes Eingreifen einer Person,
- auf Darlegung des eigenen Standpunkts, sowie
- des Rechts auf Anfechtung der Entscheidung.

In diesem Sinne regelt Art. 22 Abs. 3 DSGVO Pflichten des Verantwortlichen, sofern in den Fällen des Abs. 2 a) und c) automatisierte Einzelfallentscheidungen getroffen werden können. Da es sich um Mindestgarantien handelt, ist die Aufzählung nicht abschließend.[785] Zudem sollte ein Anspruch auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung bestehen (ErwGr. 71 S. 4 DSGVO, vgl. Abschnitt 5.2.2.3). Zur Erreichung einer „fairen und transparenten" Verarbeitung zählt ErwGr. 71 S. 6 DSGVO zudem auf: geeignete mathematische oder statistische Verfahren, Maßnahmen zur Korrektur von Faktoren, die zu unrichtigen personenbezogenen Daten führen, Minimierung des Risikos von Fehlern, Datensicherung sowie Verhinderung diskriminierender Wirkung aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung.

Besondere Kategorien: Art. 22 Abs. 4 DSGVO konkretisiert Art. 22 Abs. 2 DSGVO dahingehend, dass diese hier genannten Ausnahmen nicht auf Daten besonderer Kategorie im Sinne des Art. 9 Abs. 1 DSGVO Anwendung finden, sofern nicht besondere Umstände vorliegen.

Rechtsvorschriften in Deutschland: Im BDSG finden sich die §§ 30, 31 und 37 BDSG, die konkretisierende Regelungen zu automatisierten Einzelfallentscheidungen bspw. bei Verbraucherkrediten und Profiling enthalten. Im Beschäftigtendatenschutz gibt es keine spezielleren Regelungen.

7.1.2 Kritik

Anwendbarkeit auf Recommender- und Assistenzsysteme: Nach Ansicht der DSK, hat die Praxis gezeigt, dass Art. 22 DSGVO insbesondere auch im Beschäftigungskontext nicht ausreichend Schutz gewährleistet, da dessen Wortlaut nur automatisierte Entscheidungen verbietet.[786] Reine Entscheidungsunterstützungssysteme fallen im Grundsatz aus dem Schutzbereich der Norm, was zu Schutzlücken führen kann.[787]

---

[783] Zu beachten ist, dass es sich hierbei nicht um eine Rechtsgrundlage für die Datenverarbeitung selbst, sondern nur eine Verfahrensvorschrift handelt: *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 3 ff.; *Buchner,* in: Kühling/Buchner - DS-GVO/BDSG Art. 22 Rn. 11.

[784] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (278). m.w.N.

[785] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (280).

[786] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20220429-Besch%C3%A4ftigtendatenschutz.pdf?__blob=publicationFile&v=1 [letzter Abruf 30.05.2022], S. 2.

[787] *Horstmann/Dalmer*, ZD 2022, 260 (261); *Martini*, JZ 2017, 1017 (1020).

Die Problematik liegt in der Übernahme der Entscheidungsempfehlung eines KI-Systems. Wird ein maschinell erstellter Entscheidungsvorschlag ungeprüft übernommen, liegt trotz etwaig vorhandener Prüfungskompetenz kein relevantes menschliches Mitwirken vor[788] – ein Umstand, der allerdings nach außen für die betroffenen Personen oftmals kaum ersichtlich sein wird. Dem Vorschlag des Parlaments „vorrangig" automatisierte Entscheidungen ebenfalls zu erfassen, wurde allerdings nicht gefolgt. Das VG Wiesbaden argumentiert in seiner Vorlagefrage an den EuGH, dass eine extensive Auslegung nichtsdestotrotz möglich bleibe, nach der auch bei der automatisierten Erstellung eines Scores, welcher sodann einer Vertragsverhandlung zugrunde liegt, Art. 22 DSGVO zur Anwendung kommen könne.[789] Denn bereits die Erstellung des Scorewertes sei eine eigenständige Entscheidung, welche die anschließende (menschliche) Entscheidung in der Vertragsverhandlung derart determiniert, dass der Scorewert auf diese „durchschlägt".[790] Andernfalls entstünde eine Rechtsschutzlücke, wenn im Rahmen der am Ende rechtliche Wirkung entfaltenden Entscheidung der maschinell erstellte Scorewert nicht mehr hinterfragt wird.[791]

Die Konstellation, bei der die Entscheidung vorgelagerte Datenverarbeitung schon die eigentliche inhaltliche Bewertung der Entscheidung enthält, die finale Entscheidungsvornahme aber durch einen anderen (menschlichen) Akteur erfolgt, bietet allerdings noch einige Problemfelder: So kann der:die Entscheider*in mangels Einblicks in die Berechnungsmethoden kaum die Informations- und Auskunftsrechte im Hinblick auf die involvierte Logik erfüllen (vgl. Abschnitt 5.2.2.3), eine Anfechtung vollumfänglich prüfen der die Gewährleistung fairer Verarbeitung und Nichtdiskriminierung durch technische und organisatorische Maßnahmen sicherstellen.[792] Um einer Verantwortungsdiffusion durch Zusammenwirken mehrerer Akteure und der damit durch Automatisierung noch verschärften Problematik der Risiken der Intransparenz und Verantwortungsnegation Herr zu werden, schlagen *Horstmann/Dalmer* die konsequente Anwendung der Prinzipien der gemeinsamen Verantwortung nach Art. 26 DSGVO vor.[793] Insgesamt scheint es auch in Bezug auf sonstige KI-Systeme, deren Ergebnis eine (Vor-)Bewertung ist, die eine menschliche Letztentscheidung letztendlich vollständig determinieren, sachgerechter, dem Verantwortlichen die Aufgabe aufzuerlegen in Zusammenwirken mit der:dem KI-System-Ersteller*in die notwendigen Transparenz- und Überprüfungspflichten zu erfüllen, als den betroffenen Personen den Schutz von Art. 22 DSGVO zu versagen. Die ausstehende EuGH-Entscheidung zur Vorlagefrage des VG Wiesbaden wird insoweit Klarheit schaffen.

Umsetzung im Beschäftigungskontext: Setzt ein:e Arbeitgeber*in ein KI-System zur Vorbereitung einer Entscheidung, wie der Ablehnung einer Bewerbung oder Kündigung, etc. ein, und unterliegt diese Entscheidung einer eigenen Wertung, beschränkt Art. 22 DSGVO wie dargelegt diese Form des KI-Einsatzes nicht.[794] Wie allerdings kann das Vorliegen einer eigenen Wertung überprüft werden? Hier kommen die Beteiligungsrechte der §§ 99 Abs. 1 S. 1 bzw. 102 Abs. 1 S. 1 BetrVG ins Spiel: hier hat der:die Arbeitgeber*in den Betriebsrat darüber zu informieren, wie die Gesamtbewertung der Bewerber*innen bei personellen Einzelmaßnahmen zustande gekommen ist bzw. die Gründe der Kündigung mitzuteilen.[795] Das gilt, wie der Gesetzgeber bekräftigt, auch bei einer Personalauswahl unter Einsatz von KI.[796] Daraus wird abgeleitet, dass bereits aus §§ 99 Abs. 1 S. 1 bzw. 102 Abs. 1 S. 1 BetrVG eine Pflicht zur eigenen Wertung folge und ein bloßer Verweis auf

[788] *Horstmann/Dalmer*, ZD 2022, 260 (261).
[789] VG Wiesbaden, Beschluss vom 1.10.2021 – 6 K 788/20.
[790] VG Wiesbaden, Beschluss vom 1.10.2021 – 6 K 788/20, Rn. 25.
[791] VG Wiesbaden, Beschluss vom 1.10.2021 – 6 K 788/20, Rn. 31.
[792] *Horstmann/Dalmer*, ZD 2022, 260 (263).
[793] *Horstmann/Dalmer*, ZD 2022, 260 (263).
[794] *Frank/Heine*, NZA 2021, 1448 (1452).
[795] *Frank/Heine*, NZA 2021, 1448 (1452).
[796] Vgl. BT-Drs. 19/28899, 15.

eine KI-Bewertung nicht ausreicht.[797]

„Wenn-Dann-Entscheidungen“ vs. Persönlichkeitsbewertungen: Auf der anderen Seite wird wiederum ein zu weiter Anwendungsbereich attestiert, wenn es um einfache „Wenn-Dann-Entscheidungen“ geht.[798] So können auch bei Sachverhalten, wie dem autonomen Fahren, automatisiert getroffene Entscheidungen erhebliche Auswirkungen auf natürliche Personen haben, insbesondere wenn es zu einem Unfall kommt oder in sog. Dilemmasituationen (einer unvermeidbaren alternativen Gefährdung von Menschenleben) eine Auswahlentscheidung getroffen werden muss.[799] Allerdings ist das Schutzkonzept des menschlichen Eingreifens kaum tragfähig, wenn Entscheidungen in Bruchteilen einer Sekunde getroffen werden müssen. Eine menschliche Überprüfung wäre allenfalls nachträglich möglich. Da eine Abwägung oder Gewichtung, welche Richtung das Fahrzeug bei einer drohenden Kollision einschlägt, anhand persönlicher Merkmale der potentiellen Verkehrsopfer (wie bspw. Alter, Geschlecht, etc.) ohnehin unzulässig ist,[800] darf keine Bewertung anhand von Persönlichkeitsmerkmalen stattfinden. Es handelt sich also höchstens um eine „Wenn-Dann-Entscheidung“ in Form der automatisierten Erkennung eines Menschen, einer Sache oder eines Tieres und der Entscheidung auszuweichen – die Parameter hierfür müssen beim autonomen Fahren im Rahmen eines auf Schadensvermeidung und Schadensreduzierung ausgelegten Systems der Unfallvermeidung hinterlegt sein (vgl. § 1e Abs. 2 Nr. 2 StVG). Solche Sachverhaltsmerkmale sind keine persönlichen Merkmale.[801] Das Beispiel des Profilings impliziert eine gewisse Erheblichkeit der Entscheidung.[802] Insofern wird argumentiert, dass derartige Konstellationen nicht vom Schutzzweck des Verbots automatisierter Einzelfallentscheidungen erfasst werden.[803] Insgesamt wird daher gefordert, eine „Entscheidung“ i.S.v. Art. 22 Abs. 1 DSGVO nur dann anzunehmen, wenn ein gestaltender Akt mit abschließender Wirkung in der Außenwelt ein „Mindestmaß an Komplexität“ innewohnt.[804]

Reformanregungen: Angesichts der Unzulänglichkeiten den von bestimmten Formen von KI-basierten Entscheidungen ausgehenden Gefahren kompensierende Schutzkomponenten entgegenzusetzen, sollte der Gesetzgeber im Hinblick auf eine Weiterentwicklung des Ansatzes folgende Punkte bedenken:

Adressierung sowohl von Delegationstechnik als auch Assistenz- und Recommendersystemen

- Regulierung bis hin zum Ausschluss auch bei Vorbereitungshandlungen für rechtserhebliche Entscheidungen in besonders grundrechtssensiblen Bereichen, die bereits vom Grundprinzip nicht auf statistischen Aussagen mit Prognoseungenauigkeiten basieren sollten, bei denen aus strukturellen Gründen keine individualisierten Eingangsdaten vorliegen oder diese sich mit sensiblen Kategorien überlappen[805]
  - Identifikation sensibler Einsatzgebiete, wie bspw. strafrechtliche Verfahren
  - Situationsadäquater Einsatz: Bewertung der Gefahren diskriminierender Vorfilterung vermeintlich „neutraler“ Technik, die (menschliche) Entscheidungskorridore verengen oder durch massenhafte

[797] *Frank/Heine*, NZA 2021, 1448 (1452).
[798] Für eine Ausnahme vom Verbot: *Horstmann/Dalmer*, ZD 2022, 260 (262); *von Lewinski,* in: BeckOK DatenschutzR Art. 22 Rn. 9; *Buchner,* in: Kühling/Buchner - DS-GVO/BDSG Art. 22 Rn. 18; *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (279).
[799] Siehe hierzu: *Wagner*, Das neue Mobilitätsrecht, S. 159 f. m.w.N.
[800] Vgl. hierzu: BVerfGE 115, 118-166 – Luftsicherheitsgesetz; sowie zum autonomen Fahren: § 1e Abs. 2 Nr. 2 Buchst. c StVG.
[801] *von Lewinski,* in: BeckOK DatenschutzR Art. 22 Rn. 9.
[802] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (279).
[803] *Wagner*, Das neue Mobilitätsrecht, S. 159 f. m.w.N.
[804] *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (279); *von Lewinski,* in: BeckOK DatenschutzR Art. 22 Rn. 13; vgl. auch *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 18.
[805] Vgl. *Wischmeyer*, AöR 2018, 1 (24 ff.).

Anwendung zementieren[806]

Kennzeichnungspflichten[807]

- Kennzeichnung des Einsatzes von lernfähigen Algorithmen in persönlichkeitssensiblen Feldern
  - Bereitstellung von Klassifikationskriterien für persönlichkeitssensible Felder
  - Kennzeichnung durch visuell leicht erfassbare Symbole

Schärfung des Schutzbereichs auf die Bewertung von Persönlichkeitsmerkmalen

- Definition von Qualitätsmaßstäben[808]
- Ggf. Erweiterung auf Bereiche mit kollektiver Schadensneigung gesellschaftlicher Grundwerte (bspw. Demokratiegefährdung, Steuerung gesellschaftlicher Meinungsbildungsprozesse, Einschränkung freien Wettbewerbs) bspw. durch Etablierung eines Rechts auf Nicht-Personalisierung

7.2 Vergleich der Schutzmechanismen nach DSGVO und Entwurf einer KI-VO

7.2.1 Ethische Vorüberlegungen

Mit dem Ziel der Förderung vertrauenswürdiger KI setzte die EU-Kommission eine Hochrangige Expertengruppe zur Entwicklung ethischer Leitlinien ein. Als die drei zentralen Anforderungen an KI wurden identifiziert:[809]

- Achtung der menschlichen Autonomie
- Schadensverhütung
- Fairness und Erklärbarkeit

Die Spannungen zwischen diesen Zielen müssten bei der Entwicklung, Einführung und Nutzung von KI-Systemen zur Kenntnis genommen und gelöst werden. Zudem seien **schutzbedürftige Gruppen**, die einem hohen Exklusionsrisiko ausgesetzt sind, besonders geschützt werden. Angemessene Schutzmaßnahmen werden zudem für Situationen, die sich durch ungleiche **Macht- und Informationsverteilung** auszeichnen, und im Hinblick auf potenziell **negative gesellschaftliche Auswirkungen** auf Demokratie, Rechtsstaatlichkeit, Verteilungsgerechtigkeit oder den menschlichen Geist als solchen angemahnt. [810] Ausgehend davon, wurden weitere sieben Anforderungen für KI abgeleitet:

1. Vorrang menschlichen Handelns und menschliche Aufsicht,
2. technische Robustheit und Sicherheit,
3. Schutz der Privatsphäre und Datenqualitätsmanagement,
4. Transparenz,
5. Vielfalt, Nichtdiskriminierung und Fairness,

[806] Die „Übersetzung" sozialer Realität von Wertvorstellungen auf Grundlage einer Vergangenheitsdatenanalyse in binären Code sowie die Ableitung von Gruppenwahrscheinlichkeiten auf Einzelne bedingt die Gefahr selbstreferenzieller Entscheidungsmechaniken, welche bereits existierende strukturelle Ungleichheiten verstärkt, vgl. *Martini*, JZ 2017, 1017 (1018).
[807] *Martini*, JZ 2017, 1017 (1020).
[808] Vgl. *Wischmeyer*, AöR 2018, 1 (24).
[809] *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 2.
[810] *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 2.

6. gesellschaftliches und ökologisches Wohlergehen sowie
7. Rechenschaftspflicht.[811]

Weiterhin wird die **Technologieoffenheit** eines Regulierungsansatzes, die klare und proaktive **Informationsübermittlung** über Fähigkeiten und Grenzen von KI, Schaffung von Möglichkeiten der **Rückverfolgbarkeit** und **Nachprüfbarkeit** von KI-Systemen, die **Beteiligung** von Interessenträger*innen während des gesamten Lebenszyklus sowie Forschungs-, Schulungs- und Ausbildungsförderung zum besseren **Kompetenzaufbau** hervorgehoben.[812]

7.2.2 Aufbau des KI-VO-Entwurfs: Risikobasierter Ansatz

Da KI-Systeme in unterschiedlichsten Kontexten unter diversen Zweckbestimmungen eingesetzt werden können, differenziert der Entwurf der EU-Kommission nach den jeweils erwartbaren Risiken und clustert KI-Systeme grundsätzlich anwendungs- und domänenübergreifend in verbotene Praktiken, sog. „Hochrisiko-KI-Systeme“, sonstige Systeme mit geringem Risiko und Systemen mit minimalen Risiko, die keiner besonderen Regulierung unterliegen sollen. Anstelle eines sektoralen Ansatzes soll so ein einheitlicher, horizontaler Rechtsrahmen unabhängig vom jeweiligen Einsatz-Sektor geschaffen werden.[813] Ob personenbezogene Daten beim Einsatz des KI-Systems verarbeitet werden, ist nicht von entscheidender Relevanz – die Regelung der DSGVO soll unberührt bleiben.[814]

Unanehmbares Risko	Hochrisiko-KI-Systeme	Normales Risiko	Minimales Risiko
• Verbot bestimmter KI-Systeme mit unannehmbaren Risiko • Beispiele: manipulative Praktiken, biometrische Fernidentifizierung	• Beaufsichtigung, Transparenz-, Risiko- & Qualitätsmanagement, Dokumentations- & Nachweispflichten • Beispiele: Auswahltools für Bewerbungen	• Transparenz- & Aufklärungsregel • Beispiele: Chatbot	• keine zusätzliche Regulierung • Beispiele: Videospiele, Suchmaschinen, SPAM-Filter

Abbildung 19 Klassifikation von KI-Systemen nach COM (2021) 206 final

Der Entwurf basiert zudem auf dem „New Legislative Framework“, welcher den Ordnungsrahmen für die Europäische Produktregulierung bildet. Danach werden im Verordnungstext nur grundlegende Bausteine verbindlich vorgeschrieben, die dann weitere Konkretisierung durch europäische technische Standards erhalten und in einem nach Risiken abgestuften Konformitätsbewertungssystem aus Selbsteinschätzung und externer Prüfung durch zugelassene Stellen (vor Markteinführung) sowie staatlicher Marktüberwachung kontrolliert werden.[815]

[811] *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 3.
[812] *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 3.
[813] *Orssich*, EuZW 2022, 254 (256).
[814] Vgl. die Erläuterungen der EU-Kommission in COM(2021) 206 final.
[815] *Orssich*, EuZW 2022, 254 (256).

7.2.3 Anwendungsbereich, Definitionen & Rollenkonzept

Der Anwendungsbereich richtet sich zunächst nach der Definition des „KI-Systems“. In räumlicher Hinsicht, sollen adressiert werden:

- sämtliche Anbieter, die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen (unabhängig von der Niederlassung)
- Nutzer von KI-Systemen, die sich in der Union befinden, sowie
- in Drittland ansässige Anbieter und Nutzer von KI-Systemen, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird.

Ausnahmen sollen für KI-Systeme gelten, die Sicherheitskomponenten von Produkten oder Systemen oder selbst Produkte oder Systeme sind, welche bereits von spezielleren Verordnungen und Richtlinien erfasst werden (bspw. die Verordnung zur Typengenehmigung von Kraftfahrzeugen oder die General Safety Regulation für den Fahrzeugbereich). Ausgenommen soll zudem der militärische Bereich sowie internationale Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit sein.

Anders als die DSGVO wird keine ausdrückliche Haushaltsausnahme für den privaten Bereich von der EU-Kommission vorgesehen. Allerdings findet sich im Rahmen der Definition des „Nutzers“ die Ausnahme, dass die Nutzereigenschaft nicht greift, wenn „das KI-System […] im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet [wird]“.

7.2.3.1 Definition „System der Künstlichen Intelligenz (KI-System)“

Die von der EU-Kommission vorgeschlagene Definition setzt sich zusammen aus einer Legaldefinition der wesentlichen funktionalen Merkmale in Kombination mit Verweis auf Anhang I zu den spezifischen Techniken und Konzepten. Dies soll der Kommission die notwendige Flexibilität einräumen, über Anpassungen des Anhangs auf technologische Entwicklungen zu reagieren.[816]

> **Art. 3 Nr. 1 COM (2021) 206 final**
>
> eine **Software**, die mit einer oder mehreren der in Anhang I aufgeführten **Techniken** und **Konzepte** entwickelt worden ist und im Hinblick auf eine Reihe von *Zielen*, die vom *Menschen* festgelegt werden, **Ergebnisse** wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen *kann*, die das Umfeld **beeinflussen**, mit dem sie **interagieren**;
>
> **Anhang I Techniken und Konzepte KI**
>
> a) Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning);
>
> b) Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme;
>
> c) Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

Insgesamt wird kritisiert, dass die aufgelisteten Techniken zu weit greifend ausgefallen sind.[817] Die Definition

[816] Vgl. ErwGr. 6 KI-VOE.
[817] *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188 (1189); *Europäischer Wirtschafts- und Sozialausschuss/Christa Schweng*, Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses, vom 22.12.2021 2021/C 517/09, S. 2.;

droht dadurch konturlos und ausufernd zu geraten. Die Definition basiert auf den Erwägungen der Kommission im Weißbuch[818] und einer Mitteilung über KI für Europa:[819]

> „Künstliche Intelligenz (KI) bezeichnet Systeme mit einem „intelligenten" Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen. KI-basierte Systeme können rein softwaregestützt in einer virtuellen Umgebung arbeiten (z. B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme), aber auch in Hardware-Systeme eingebettet sein (z. B. moderne Roboter, autonome Pkw, Drohnen oder Anwendungen des ‚Internet der Dinge')."

Mit dem Verweis auf „Intelligenz" konnte dieser Ansatz nicht überzeugen.[820] Daraufhin erfolgte eine Präzisierung der Hochrangigen Expertengruppe:

> „Künstliche-Intelligenz-(KI)-Systeme sind vom Menschen entwickelte Software- (und möglicherweise auch Hardware-) Systeme, die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene agieren, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten und über die geeignete(n) Maßnahme(n) zur Erreichung des vorgegebenen Ziels entscheiden. KI-Systeme können entweder symbolische Regeln verwenden oder ein numerisches Modell erlernen, und sie können auch ihr Verhalten anpassen, indem sie analysieren, wie die Umgebung von ihren vorherigen Aktionen beeinflusst wird."[821]

Die verschiedensten Definitionsversuche[822] zeigen allerdings die Schwierigkeit, aufbauend auf dem bereits kaum definierbaren Konzept der „Intelligenz" eine tragfähige Definition zu finden. Es kann daher nur empfohlen werden, weniger auf das Sammelbecken an Technologien zu rekurrieren, sondern die herausragenden, risikoverursachenden Charakteristika zu benennen, zuvörderst die Aspekte der (eigenständigen) Entscheidung und Lernfähigkeit.[823]

7.2.3.2 „Hochrisiko-KI"

Der zentrale Fokus des Entwurfs liegt auf den Hochrisiko-Systemen. Auch dieser Klassifikationsansatz soll sich nach dem Konzept der EU-Kommission aus der Kodifikation von Bedingungen und Auflistung von Bereichen im Anhang zusammensetzen. Danach sollen erfasst werden:

- KI-Systeme, die als Sicherheitskomponente eines Produkts verwendet werden sollen oder selbst ein solches Produkt sind, das unter die in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union fällt und einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme unterzogen werden muss,
- KI-Systeme in Anhang III aus den Bereichen:
  - Biometrische Identifizierung / Kategorisierung
  - Kritische Infrastrukturen
  - Zugang zu allgemeiner / beruflicher Bildung sowie bestimmte Bewertungssysteme
  - Beschäftigung, Personalmanagement / Zugang zur Selbstständigkeit

---

Bundesverband der Deutschen Industrie e.V. (BDI), BDI-Stellungnahme zum Entwurf einer europäischen KI-Verordnung, S. 3; *Ebers u. a.*, RDi 2021, 528 (529).; BR-Drs. 488/21, S. 7.

[818] *EU-Kommission,* Weißbuch Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Brüssel, den 19.2.2020, COM(2020) 65 final, S. 19.

[819] EU-Kommission, Mitteilung zu „Künstliche Intelligenz für Europa" vom 25.04.208, COM(2018) 237 final, S. 1.

[820] Zur Kritik: *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. I 1.

[821] *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, S. 47.

[822] Siehe bspw. die Übersicht bei: *Kaulartz/Braegelmann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. I 1.

[823] Vgl. hierzu: Abschnitt 1.

- Zugang und Inanspruchnahme zu grundlegenden privaten / öffentlichen Diensten / Leistungen
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

7.2.3.3 Rollen

Anders als die DSGVO kennt der Kommissionsentwurf keine von der KI-Entscheidung betroffene Person.[824] Folglich sind auch keine Betroffenenrechte vorgesehen. Damit fehlt ein wesentliches Element, um auf die Umsetzung des Pflichtenkanons hinzuwirken. So wird zwar der „Nutzer" aufgeführt, aus datenschutzrechtlicher Perspektive kann es sich hierbei um die betroffene Person, aber auch um den Verantwortlichen handelt, der mit Hilfe des KI-Systems personenbezogene Daten verarbeitet.

- **„Nutzer"** natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet (Ausnahme: persönliche und nicht berufliche Tätigkeit)
- **„Anbieter"** eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen
- **„Einführer"** in der Union ansässige / niedergelassene natürliche oder juristische Person, die ein KI-System unter fremder Marke in der Union in Verkehr bringt oder in Betrieb nimmt
- **„Händler"** eine natürliche oder juristische Person in der Lieferkette, die ein KI-System ohne Änderung seiner Merkmale auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers
- **„Bevollmächtigter"** vom Anbieter eines KI-Systems schriftlich dazu bevollmächtigt wurde, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen

Bei Anbieter, Nutzer, Bevollmächtigtem, Einführer und Händler handelt es sich um **„Akteure".**

7.2.4 Schutzmechanismen

Neben den in Art. 5 KI-VOE geregelten verbotenen Praktiken, widmen sich die Großzahl an Regelungen den „Hochrisiko-KI-Systemen". Diese Schutzmechanismen sollen im Folgenden mit den Anforderungen der DSGVO gegenübergestellt werden.

7.2.4.1 Menschliche Aufsicht

Sowohl im Rahmen einer ausnahmsweise erlaubten automatisierten Einzelfallentscheidung nach Art. 22 DSGVO als auch in Art. 14 KI-VOE wird die Aufsicht durch einen Menschen als Schutzkonzept etabliert.

Art. 22 DSGVO	Entwurf KI-VO
• der Verantwortliche trifft **angemessene Maßnahmen, um die Rechte und Freiheiten** sowie	• **Hochrisiko-KI-Systeme** werden so konzipiert und entwickelt, dass sie während der Dauer der

[824] *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Gemeinsame Stellungnahme 5/2021 zum 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, S. 10.

die berechtigten Interessen der betroffenen Person zu wahren, wozu • **mindestens das Recht auf Erwirkung des Eingreifens einer Person** seitens des Verantwortlichen, • auf **Darlegung des eigenen Standpunkts** und • auf **Anfechtung der Entscheidung** gehört.	Verwendung des KI-Systems – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen **wirksam beaufsichtigt** werden können. • Einbezug **vorhersehbarer Fehlanwendung** • Menschliche Aufsicht „eingebaut“ oder von Nutzer umsetzbar • Maßnahmen, welche menschliche Aufsicht ermöglichen, u.a. Fähigkeit Grenzen des Systems zu **verstehen**, „Stopptaste“ / Abschaltbar, Neigung **übermäßigem Vertrauen entgegenwirken** („Automatisierungsbias“), richtiges Interpretieren

7.2.4.2 Risikomanagement

Zunächst erfolgt im KI-VOE die Auflistung verbotener Praktiken in Art. 5 KI-VOE. Hierzu zählen vor allem:

- Systeme der unterschwelligen Beeinflussung zur Verhaltensbeeinflussung, sofern dadurch ein Schaden entstehen kann
- Ausnutzung der Schwäche oder Schutzbedürftigkeit durch Alter oder körperliche/geistige Behinderungen, sofern dadurch ein Schaden entstehen kann
- Systeme zur Klassifizierung der Vertrauenswürdigkeit natürlicher Personen gegenüber Behörden mit der Gefahr der ungerechtfertigten, unverhältnismäßigen oder unsachgemäßen Schlechterstellung oder Benachteiligung
- biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (mit Ausnahmen)

Für Hochrisiko-KI-Systeme enthält Art. 9 KI-VOE Regelungen zum Risikomanagementsystem, welches einzurichten und zu dokumentieren ist, wobei sich dies als kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems versteht, der eine regelmäßige systematische Aktualisierung erfordert. Art. 17 KI-VOE enthält zusätzlich die Pflicht zur Einrichtung eines Qualitätsmanagementsystems.

Art. 22, 35 DSGVO	Entwurf KI-VO
• **Datenschutz-Folgenabschätzung** bei: „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf **automatisierte Verarbeitung** einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die **Rechtswirkung** gegenüber natürlichen Personen entfalten oder diese in ähnlich **erheblicher Weise beeinträchtigen**“ → Abhilfemaßnahmen zur Bewältigung der Risiken oder Konsultation Aufsichtsbehörde	• **Risikomanagementsystem** • Gesamten Lebenszyklus: Risiken einschätzen und Abhilfemaßnahmen • je Zweckbestimmung „vertretbare“ Risiken • **Qualitätsmanagementsystem**, u.a.: • Konzept zur Einhaltung einschlägiger Regulierungsvorschriften • Untersuchungs-/Test-/Validierungsverfahren

	• Datenmanagement • System zur Beobachtung nach Inverkehrbringen • Dokumentation & Kommunikation mit Behörden

7.2.4.3 Transparenz

Die KI-VOE enthält unterschiedliche Regelungen zur Transparenz für Hochrisiko-KI-Systeme und sonstige KI-Systeme. Während nach DSGVO über Informations- und Auskunftsrechte die Datenverarbeitung gegenüber der *betroffenen Person* nachvollziehbar gemacht werden soll, bezieht sich Art. 13 KI-VOE auf den „*Nutzer*“ und „*Anbieter*“ des KI-Systems. Die Nutzer*innen sollen die Ergebnisse des Systems angemessen interpretieren und verwenden können. Die auf „geeignete Art“ und „in angemessenem Maß“ gewährleistete Transparenz soll es Nutzer*innen und Anbieter*innen ermöglichen ihre Pflichten nach KI-VOE erfüllen zu können. Hierfür sollen Hochrisiko-KI-Systeme mit einer Gebrauchsanweisung versehen werden, die Informationen für die Nutzer*innen relevanten, barrierefrei zugänglichen und verständlichen Form enthalten.

Art. 13, 22 DSGVO	Entwurf KI-VO

• **Datenschutzerklärung**
  • Hinweis auf das Bestehen einer automatisierten Entscheidungsfindung
  • aussagekräftige Informationen über die **involvierte Logik** sowie die **Tragweite** und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
	• *A. Hochrisiko-KI:*
	  • „Hinreichende“ Transparenz mit Mindestinformationen, u.a. Leistungsgrenzen, Genauigkeit, Sicherheit
	  • **Gebrauchsanweisung**
	• *B. „Normale“ KI:*
	  • KI-System, insbesondere Deepfakes, Emotionserkennung oder biometrische Kategorisierung als solche kenntlich machen

7.2.4.4 Dokumentation und Nachweispflichten

Potenzielle Rechtsverstöße überprüfen zu können, setzt eine effektive Beweissicherung voraus – *Martini* bemängelt allerdings, dass bspw. die DSGVO-Pflicht zur Pflege eines Verzeichnisses von Verarbeitungstätigkeiten hinter dieser Anforderung zurückbleibt, da nur Elementardaten verzeichnet werden, nicht hingegen Programmabläufe und Entscheidungsparameter.[825] Während nach DSGVO Dokumentations- und Nachweispflichten vor allem aus der Rechenschaftspflicht folgen, enthalten Art. 11 und 12 KI-VOE detaillierte Vorgaben zur technischen Dokumentation, die vor Inverkehrbringen oder Inbetriebnahme zu erstellen ist, und zu Aufzeichnungspflichten, die die automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung“) während des Betriebs der Hochrisiko-KI-Systeme ermöglichen. Die Protokollierung soll gewährleisten, dass das Funktionieren des KI-Systems während seines gesamten Lebenszyklus in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar ist.

[825] *Martini*, JZ 2017, 1017 (1022).

Art. 22, 24 DSGVO	Entwurf KI-VO

• Ggf. Verzeichnis von Verarbeitungstätigkeiten
• Allgemeiner Grundsatz: **Rechenschaftspflicht**
  • Der Verantwortliche ist für die Einhaltung der DSGVO verantwortlich und muss deren Einhaltung nachweisen können
	• **Technische Dokumentation**
	  • Dient Nachweis zur Einhaltung Pflichten der KI-VO; Mindestangaben
	• **Aufzeichnungspflichten**
	  • Protokollierung während Betrieb
	  • Dient Überwachung Betrieb

7.2.4.5 Daten und Daten-Governance

Gerade die Qualitätssicherung der Trainings-, Validierungs- und Testdaten stellt einen wichtigen Baustein für nicht-diskriminierende und produktive KI-Systeme dar.[826] Daher fordert Art. 10 KI-VOE geeignete Daten-Governance- und Datenverwaltungsverfahren, insbesondere zu konzeptionellen Entscheidungen, Datenerfassung, Datenaufbereitungsvorgängen, Annahmen und Bewertungen, Untersuchung möglicher Verzerrungen (Bias) sowie Ermittlung möglicher Datenlücken.

Art. 5, 16 DSGVO	Entwurf KI-VO

– Grundsatz der Richtigkeit
  ○ Berichtigungs-/Löschpflichten
  ○ Berichtigungsanspruch
  ○ Vervollständigung unvollständiger Daten
	– Daten-Governance- und Datenverwaltungsverfahren: Trainings-, Validierungs- und Testdaten müssen Qualitätskriterien entsprechen
	– Daten relevant, repräsentativ, fehlerfrei und vollständig
	– besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen des Einsatzwecks entsprechen

Soweit dies für die Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist, dürfen die Anbieter*innen solcher Systeme besondere Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen (Art. 10 Abs. 5 KI-VOE). Hierzu zählen auch technische Beschränkungen einer Weiterverwendung und modernste Sicherheits- und Datenschutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung, wenn der verfolgte Zweck durch eine Anonymisierung erheblich beeinträchtigt würde.

7.2.4.6 Cybersicherheit

Art. 15 KI-VOE adressiert die Genauigkeit, Robustheit und Cybersicherheit von Hochrisiko-KI-Systemen. Gefordert wird ein „angemessenes Maß“ im Hinblick auf die Zweckbestimmung.

Art. 32 DSGVO	Entwurf KI-VO

[826] *Wischmeyer*, AöR 2018, 1 (23).

– Datensicherheit ○ Geeignete TOMs zur Gewährleistung dem Risiko angemessenes Schutzniveau	– Angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit während gesamten Lebenszyklus – Angabe Genauigkeitsgrade in Gebrauchsanweisung – Widerstandsfähig ggü. Fehlern / Störungen (z.B. durch technische Redundanz) – Risikominderungsmaßnahmen für Rückkopplungsschleifen – Risiko angemessene Cybersicherheit

Für im Einsatz dazulernende Hochrisiko-KI-Systeme sind angemessene Risikominderungsmaßnahmen gegenüber Rückkopplungsschleifen vorzusehen, d.h. möglicherweise verzerrte Ergebnisse, die durch eine Verwendung vorheriger Ergebnisse als Eingabedaten für den künftigen Betrieb entstehen (Art. 15 Abs. 3 KI-VOE). Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen zur Verhütung und Kontrolle von Angriffen, mit denen versucht wird, den Trainingsdatensatz zu manipulieren („Datenvergiftung“), von Eingabedaten, die das Modell zu Fehlern verleiten sollen („feindliche Beispiele“), oder von Modellmängeln (Art. 15 Abs. 4 KI-VOE).

7.2.4.7 Formelle Anforderungen

Können Einzelne insbesondere aufgrund von Macht- und Informationsasymmetrien kaum Einfluss nehmen, um ihre Rechte wahrzunehmen, bedarf es kollektiver Kontrollmechanismen, wie staatliche Kontrollverfahren oder einen „Algorithmen-TÜV“.[827] Diese können präventiv, ex-post oder parallel zum Produktlebenszyklus ansetzen und sowohl repressiv als auch selbstregulativ ausgestaltet sein.[828] Das Konzept der Zertifizierung in der DSGVO beruht auf dem Gedanken der Freiwilligkeit, um als Faktor im Rahmen der Nachweispflichten herangezogen zu werden. Der KI-VOE sieht dagegen unterschiedliche Verfahren der Bewertung, Bescheinigung und Kennzeichnung der Konformität der Hochrisiko-KI-Systeme vor. Flankiert wird dies mit Meldepflichten sowie der Einrichtung einer EU-Datenbank.

DSGVO	Entwurf KI-VO
Faktor zum Nachweis der Einhaltung der DSGVO-Anforderungen durch Zertifizierung, Art. 42 DSGVO (keine Verpflichtung)	– Konformitätsbewertung – Konformitätsbescheinigung – EU-Konformitätserklärung – CE-Konformitätskennzeichnung – Meldepflichten – Registrierung in EU-Datenbank

7.2.4.8 Prozesse, interne und externe Aufsicht

Ähnlich dem Europäischen Datenschutzausschuss soll ein Europäischer Ausschuss für künstliche Intelligenz

[827] *Martini*, JZ 2017, 1017 (1021).
[828] *Martini*, JZ 2017, 1017 (1021).

eingerichtet werden (Art. 56 ff. KI-VOE). Zudem sollen notifizierte Stellen als Konformitätsbewertungsstellen und notifizierte Behörden benannt werden (Art. 30 ff. KI-VOE). Diese sollen als Aufsichtsbehörden auch die Marktüberwachung übernehmen, es sei denn im Mitgliedstaat fungieren hierfür unterschiedliche Behörden (Art. 59 KI-VOE).

DSGVO, BDSG, BetrVG	Entwurf KI-VO
– Aufsichtsbehörden – Datenschutzbeauftragte – Mitbestimmungsrechte Betriebsrat	– Notifizierte Konformitätsbewertungsstelle – nationale Aufsichtsbehörde als notifizierte Behörde zur Überwachung der Konformitätsbewertungsstellen und Marktüberwachungsbehörde

7.3 Zwischenergebnis zu KI-Entscheidungen und Datenschutz

Der Anwendungsbereich des Verbots von automatisierten Einzelfallentscheidungen in Art. 22 DSGVO ist noch begrenzt und durch Ausnahmen aufgeweicht. Als Schutzmechanismus ist die Anfechtbarkeit und das Einschreiten eines Menschen vorgesehen. Weitere Schutzmechanismen der DSGVO knüpfen gesteigerte Anforderungen an die Automatisierung der Entscheidung oder Profiling. So ist im Hinblick auf die Transparenz über die involvierte Logik zu informieren bzw. Auskunft zu erteilen und im Hinblick auf gesteigerte Risiken regelmäßig eine DSFA durchzuführen. Überschneidungen zu den geplanten Schutzkonzepten des Kommissionsentwurfs einer KI-Verordnung sind bei Hochrisiko-KI-Systemen möglich. Diese sollen künftig zahlreichen Anforderungen unterliegen, wobei sich diese wiederum in einige bereits aus dem Datenschutz bekannte Aspekte wie Dazwischentreten eines Menschen, Risikomanagement, Transparenz, Dokumentation und Nachweispflichten, Daten-Governance/Richtigkeit und Cybersicherheit clustern lassen. KI-Systeme mit einem unannehmbaren Risiko sollen hingegen verboten werden. Für sonstige KI-Systeme ist nur eine Transparenzregel vorgesehen. Allerdings bestehen noch erhebliche Diskussionen insbesondere zur vorgeschlagenen Definition des KI-Systems. Es bleibt daher abzuwarten, wie sich das weitere Verfahren entwickelt und welche Überschneidungen und Unterschiede letztlich zur DSGVO etabliert werden, welche bei der Prüfung der Rechtskonformität künftig zu beachten sein werden.

Um zu prüfen, ob das Verbot der automatisierten Einzelfallentscheidung nach Art. 22 DSGVO greift, müssen folgende Fragen beantwortet werden:

- Wird eine **Entscheidung ausschließlich automatisiert** getroffen? Falls ein Mensch entscheidend: liegt eine eigenständige Überprüfung vor?
- Folgt aus der Entscheidung eine **rechtliche Wirkung** oder eine **erhebliche Beeinträchtigung** für natürliche Personen?
- Besteht eine Ausnahme vom Verbot?
  - **Ausdrückliche** Einwilligung oder **Vertrag**
    - ➢ Welche Schutzmaßnahmen wurden getroffen? Besteht für betroffene Personen die Möglichkeit das **Eingreifen einer Person** zu erwirken, den eigenen **Standpunkt darzulegen** und die Entscheidung **anzufechten**?
  - Zulässigkeit nach **Rechtsvorschrift** der Union/eines Mitgliedstaates (sofern Vorschrift angemessene Schutzmaßnahmen vorgibt)
- Beruht die Entscheidung auf der Verarbeitung **besonderer Kategorien** personenbezogener Daten?

- Liegt eine ausdrückliche Einwilligung oder legitimierende Rechtsvorschrift der Union/eines Mitgliedstaates vor?
- Welche zusätzlichen Schutzmaßnahmen wurden getroffen?

— 2. Teil: Arbeit und Lernen

8 Beschäftigtendatenschutz

Trotz mehrfacher Anregungen ein ausdifferenziertes Beschäftigtendatenschutzrecht zu kodifizieren,[829] beschränkt sich die aktuelle Rechtslage auf die Generalklausel in § 26 BDSG. Der vom Bundesministerium für Arbeit und Soziales (BMAS) eingesetzte interdisziplinäre Beirat Beschäftigtendatenschutz kommt in seinem 2022 vorgelegten Abschlussbericht zum Schluss, dass – neben weiteren Maßnahmen – ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.[830] Dies erkennt auch die aktuelle Regierungskoalition an, die im Koalitionsvertrag festgehalten hat:

> *„Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen.“*[831]

Ein Schwerpunkt der von der DSK geforderten Neuregelungen soll den Einsatz algorithmischer Systeme wie KI-Anwendungen im Beschäftigungskontext adressieren.[832]

8.1 Regelungsbefugnis im Rahmen der Öffnungsklausel des Art. 88 DSGVO

Die DSGVO bildet auch für den Beschäftigtendatenschutz das zentrale Rahmenwerk, überlässt Konkretisierungen allerdings den Mitgliedstaaten und Kollektivvereinbarungen. Für die Verarbeitung personenbezogener Daten der Beschäftigten durch ihre Arbeitgeber*innen enthält die DSGVO in Art. 88 DSGVO eine Öffnungsklausel für mitgliedstaatliches Recht. In der Literatur wird diskutiert, wie weit die Kompetenz der nationalen Gesetzgeber reicht, also insbesondere welchen Gestaltungsspielraum diese Öffnungsklausel bietet.[833]

> **Art. 88 Abs. 1 DSGVO** Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, [...] vorsehen.

Dies betrifft insbesondere folgende Aspekte:

- Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften

[829] Zuletzt erneut in der Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20220429-Besch%C3%A4ftigtendatenschutz.pdf?__blob=publicationFile&v=1 [letzter Abruf 30.05.2022].

[830] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 6, 9.

[831] Koalitionsvertrag „Mehr Fortschritt wagen“, S. 14.

[832] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, S. 2.

[833] Zur Diskussion siehe *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG Art. 88 Rn. 30 ff. m.w.N.

oder durch Kollektivvereinbarungen festgelegten Pflichten,

- des Managements, der Planung und der Organisation der Arbeit,
- der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz,
- des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie
- für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses

Mitgliedstaatliche Normen, die von dieser Regelungsoption Gebrauch gemacht haben, gehen in diesem Bereich den Vorschriften der DSGVO vor – auch wenn sich dies nicht aus der Regelung selbst ergibt, so doch aus dem Sinn und Zweck.[834] Weitere Impulse gibt die DSGVO den Mitgliedstaaten für die Umsetzung der Öffnungsklausel im 2. Absatz mit:

Art. 88 Abs. 2 DSGVO Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

Parallel bleiben aber die übrigen, allgemeinen Bestimmungen der DSGVO weiter anwendbar.[835] Zudem sind die mitliedstaatlichen Regelungen im Lichte der DSGVO EU-rechtskonform auszulegen.[836] Insofern können die Anforderungen der DSGVO im Bereich des Beschäftigtendatenschutzes als „Mindeststandard“ bezeichnet werden.[837]

8.2 Definition der Beschäftigten

Der persönliche Anwendungsbereich wird durch die Definition des Beschäftigten in § 26 Abs. 8 BDSG determiniert. Diese Aufzählung ist abschließend.[838]

§ 26 Abs. 8 BDSG

Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu

[834] *Riesenhuber,* in: BeckOK DatenschutzR Art. 88 Rn. 16.
[835] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 20.
[836] *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 4.
[837] *Dietrich u. a.*, DuD 2021, 5 (7).
[838] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 7; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 28.

diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

Arbeitnehmer*in i.S.d. § 26 Abs. 8 BDSG ist, wer sich vertraglich zu weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit gegen Vergütung verpflichtet hat.[839] Dieser Begriff folgt aus § 611a Abs. 1 BGB zum Arbeitsvertrag.[840]

§ 611a Abs. 1 BGB Durch den Arbeitsvertrag wird der Arbeitnehmer im Dienste eines anderen zur Leistung weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet. Das Weisungsrecht kann Inhalt, Durchführung, Zeit und Ort der Tätigkeit betreffen. Weisungsgebunden ist, wer nicht im Wesentlichen frei seine Tätigkeit gestalten und seine Arbeitszeit bestimmen kann. Der Grad der persönlichen Abhängigkeit hängt dabei auch von der Eigenart der jeweiligen Tätigkeit ab. Für die Feststellung, ob ein Arbeitsvertrag vorliegt, ist eine Gesamtbetrachtung aller Umstände vorzunehmen. Zeigt die tatsächliche Durchführung des Vertragsverhältnisses, dass es sich um ein Arbeitsverhältnis handelt, kommt es auf die Bezeichnung im Vertrag nicht an.

Die Reichweite ist bewusst weit gewählt, sodass alle in Abhängigkeit stehende Beschäftigten von arbeitnehmerähnlich Beschäftigten, über Auszubildende bzw. zur Arbeitserprobung am Berufsleben Teilnehmende, Leiharbeiter*innen bis hin zu leitenden Angestellten erfasst werden.[841] Zudem erfolgte eine Ausdehnung auf das Vorfeld einer Beschäftigung, d.h. das Stadium der Bewerbung, sowie die Zeit nach der Beendigung des Beschäftigungsverhältnisses. Diese weite Definition ist nicht ohne Kritik geblieben, da Bedenken aufgeworfen wurden, ob hiermit die Reichweite der Öffnungsklausel des Art. 88 DSGVO überschritten wird.[842] Andererseits präferiert auch der EuGH eine weiten Arbeitnehmerbegriff.[843] Ausschlaggebend ist danach die das Rechtsverhältnis prägende Rechte- und Pflichtenstruktur, insbesondere *„dass jemand während einer bestimmten Zeit für einen anderen nach dessen Weisungen Leistungen erbringt, für die er als Gegenleistung eine Vergütung erhält“.*[844]

Weiterhin umstritten ist, ob auch Organmitglieder, wie Geschäftsführer*innen einer GmbH oder Vorstandmitglieder einer AG, als Beschäftigte gelten sollten.[845] Hier wird argumentiert, dass diese auf Grundlage freier Dienstverträge i.S.d. § 611 BGB und nicht im Rahmen eines Arbeitsvertrags tätig werden.[846] Sie werden eher der Arbeitgeberseite als der Arbeitnehmerseite zugeordnet.[847] Andererseits können auch freie Dienstverträge unter die weite Definition des EuGH subsumiert werden.[848] Sollten diese Personen nicht unter die Regelungen des § 26 BDSG fallen, verbliebe der Rückgriff auf Art. 6 Abs. 1 Buchst. b und f DSGVO. Im Rahmen der Interessenabwägung wäre es in diesem Fall sicherlich nicht abwegig, auch das Interesse einer einheitlichen Rechtsanwendung im Betrieb als berechtigtes Interesse anzuerkennen.

[839] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 22.
[840] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 7.
[841] *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 14; *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 22.
[842] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 6.
[843] EuGH, Urteil vom 11.11.2015 – C-422/14– Pujante Rivera, Rn. 29; EuGH, Urteil vom 9.7.2015 – C-229/14 – Balkaya, Rn. 34; EuGH, Urteil vom 13.02.2014 – C-596/12 – Kommission/Italien, Rn. 17.
[844] EuGH, Urteil vom 11.11.2015 – C-422/14 – Pujante Rivera, Rn. 29.
[845] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 22.
[846] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 7.
[847] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 104.
[848] Vgl. EuGH, Urteil vom 11.11.2010 – C-232/09 – Danosa, Rn. 29; EuGH, Urteil vom 9.7.2015 – C-229/14, NJW 2015, 2481 Rn. 32 f. – Balkaya; EuGH, Urteil vom 13.02.2014 – C-596/12 – Kommission/Italien, Rn. 17.

8.3 Verantwortlichkeit

Im unternehmerischen Kontext ist der datenschutzrechtliche Verantwortliche zunächst das Unternehmen selbst.[849] Organisatorisch und im operativen Betrieb liegt die Aufgabe jedoch bei den Beschäftigten, da diese i.d.R. selbst diejenigen sind, die personenbezogene Daten verarbeiten.

Bei der Nutzung von KI-Systemen im Unternehmenskontext stellt sich die Frage, ob sich abhängig vom jeweiligen Kontext, eine Verschiebung der datenschutzrechtlichen Verantwortlichkeit bei der Nutzung von KI-Systemen ergeben könnte. Um zu beurteilen, welche datenschutzrechtlichen Verantwortlichkeiten bei dem Unternehmen, dem Dienstanbieter oder auch bei den Beschäftigten selbst liegen könnten, ist es zweckmäßig verschiedene klar abgrenzbare Fallgruppen zu bilden.

- Anordnung zur Nutzung eines KI-Systems
- Entwicklung und Betrieb eines eigenen KI-Systems
- Duldung von KI-Systemen im Rahmen einer betrieblichen Übung

8.3.1 Zurechnung des Verhaltens der Beschäftigten

Ob die Verantwortung i.S.d. Art. 4 Nr. 7 DSGVO beim Unternehmen liegt oder ausnahmsweise bei dem tatsächlich handelnden Beschäftigten, hängt davon ab, ob das Verhalten der Beschäftigten dem Unternehmen zuzurechnen ist. Hierbei ist entscheidend, ob die Datenverarbeitung zu Unternehmenszwecken oder eigenen Zwecken der Beschäftigten erfolgt. Letzterer Fall wird auch als sog. „Mitarbeiterexzess“ bezeichnet.[850] Das Unternehmen kann allerdings eine (Mit-)Verantwortung treffen. Von der Verantwortlichkeit des Arbeitgebers ist daher auszugehen, wenn die Verarbeitungstätigkeiten im Verantwortungsbereich des Unternehmens erfolgen.[851] Die Beschäftigten handeln daher in der Regel im Auftrag des Unternehmens als Arbeitgeber, sofern sie im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten.

8.3.2 Der Mitarbeiterexzess

Soweit Beschäftigte im Rahmen der tatsächlichen Möglichkeit zur Datenverarbeitung das rechtlich Erlaubte überschreiten und Daten zu eigenen Zwecken verarbeiten, handeln sie damit nicht mehr im Auftrag des Arbeitgebers und werden selbst zum Verantwortlichen.[852] Die DSK definiert diesen Mitarbeiterexzess als „Handlung von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden kann“.[853] Es soll somit nicht primär darauf ankommen, ob die Beschäftigten subjektiv eigene Interessen verfolgen, sondern ob die Zweckbestimmung objektiv betrachtet den zugewiesenen Aufgaben entspricht.[854]

Ein Mitarbeiterexzess kann für das Unternehmen als Arbeitgeber*in verschiedene Folgen haben: Zum einen

[849] Diese haften grundsätzlich für schuldhafte Datenschutzverstöße ihrer Beschäftigten: *DSK - Datenschutzkonferenz*, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019, S. 1; *Rohrlich*, ZAP 2020, 1265 (1267); *Bertram/Falder*, ArbRAktuell 2021, 95 (95); *Dury*, ZD-Aktuell 2020, 04405.
[850] Ausführlich: *Ambrock*, ZD 2020, 492.
[851] *Jung/Hansch*, ZD 2019, 143 (145); *DSK - Datenschutzkonferenz*, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019.
[852] *Ambrock*, ZD 2020, 492; *Jung/Hansch*, ZD 2019, 143 (145).
[853] *DSK - Datenschutzkonferenz*, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019, S. 1.
[854] *Ambrock*, ZD 2020, 492 (493).

kann ein Datenschutzverstoß, der öffentlich bekannt wird, mit einem Imageschaden einhergehen. Zum anderen geraten Arbeitgeber*innen in die Position, ihre organisatorischen Maßnahmen rechtfertigen zu müssen, damit sich der Beschäftigte nicht darauf berufen kann, dass er / sie lediglich im Rahmen des Erlaubten bzw. im Rahmen der zugewiesenen Tätigkeit gehandelt habe. Arbeitgeber*innen als primärer Haftungsadressaten bzw. Adressaten eines Bußgeldverfahrens[855] müssen somit einen Entlastungsbeweis führen, dass ihre Beschäftigten im Exzess als eigene Verantwortliche gehandelt haben. Datenabrufe durch Beschäftigte im Exzess sind zudem meldepflichtige Datenschutzverstöße gemäß Art. 33 DSGVO, die in der Regel der Datenschutzbehörde mitzuteilen sind.

8.3.3 Verantwortlichkeit durch Entstehung einer betrieblichen Übung

Fehlen Regelungen zur Einführung neuer Technologien im Betrieb, besteht die Gefahr, dass Ansprüche aus einer „betrieblichen Übung“ geltend gemacht werden könnten.[856] Von einer betrieblichen Übung spricht man bei einer regelmäßigen Wiederholung bestimmter Verhaltensweisen, aus denen die Beschäftigten schließen können, eine Leistung oder Vergütung solle auf Dauer gewährt werden.[857] Eine solche wiederholte Leistung kann aus einer neutralen Perspektive dahingehend gewertet werden, dass Arbeitgeber*innen stillschweigend eine Ergänzung des Arbeitsvertrags einräumen, welche die Beschäftigten ebenso stillschweigend annehmen.[858] Das BAG hat bereits Duldungen eines bestimmten Verhaltens darunter gefasst.[859] Wann und wie weit im Einzelfall solche Ansprüche abgeleitet werden können, ist allerdings umstritten. [860] Dies betrifft vor allem die Nutzung dienstlicher IT-Infrastruktur zu privaten Zwecken. Der Duldung muss ein rechtsgeschäftlicher Erklärungswert beigemessen werden können, welcher voraussetzt, dass Arbeitgeber*innen Kenntnis von der privaten Nutzung haben.[861] In der Praxis wird daher empfohlen Regelungen zum Umgang mit digitalen Technologien im Unternehmen aufzustellen.[862]

8.4 Rechtsgrundlagen für die Datenverarbeitung im Beschäftigungskontext

8.4.1 Einwilligung im Arbeitsverhältnis

Das Erteilen einer Einwilligung im Arbeitsverhältnis weist einige Besonderheiten auf. ErwGr.155 DSGVO räumt den Mitgliedstaaten insofern die Möglichkeit ein, Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen zu erlassen.[863]

---

[855] *Ambrock*, ZD 2020, 492.
[856] *Schrey u. a.*, MMR 2017, 736 (737); *Brink/Schwab*, ArbRAktuell 2018, 111 (113). Vgl. auch zur Duldung privater Nutzung betrieblicher Infrastruktur: *DSK - Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 4.
[857] BAG, Urteil vom 11. 4. 2006 - 9 AZR 500/05, Rn. 14; *Schrey u. a.*, MMR 2017, 736 (737); *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[858] BAG, Urteil vom 11. 4. 2006 - 9 AZR 500/05, Rn. 14; *Schrey u. a.*, MMR 2017, 736 (737).
[859] BAG, Urteil vom 11. 4. 2006 - 9 AZR 500/05, Rn. 14.
[860] *Schrey u. a.*, MMR 2017, 736 (737 f.); gegen die Folgerung aus bloßer Duldung: *Riesenhuber,* in: *Wolff/Brink*, BeckOK DatenschutzR, § 26 BDSG Rn, 170.
[861] LAG Berlin-Brandenburg, Urteil vom 14.01.2016 - 5 Sa 657/15, Rn. 85.
[862] *Schrey u. a.*, MMR 2017, 736 (738); *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[863] Vgl. BT-Drs. 18/11325, S. 97.

8.4.1.1 Materielle Voraussetzungen

§ 26 Abs. 2 BDSG ergänzt und konkretisiert die DSGVO-Vorschriften zur Einwilligung in Artt. 4 Nr. 11, 6 Abs. 1 Buchst. a und Art. 7 sowie Art. 8 und Art. 9 Abs. 2 Buchst. a DSGVO.

> **§ 26 Abs. 2 S. 1, 2 BDSG**
>
> Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.
>
> Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Aufgrund der abhängigen Stellung der Beschäftigten ist die Möglichkeit einer Einwilligung im Beschäftigtenkontext rechtspolitisch höchst umstritten.[864] § 26 Abs. 2 BDSG versucht diesen Bedenken Rechnung zu tragen, da besondere Beurteilungskriterien für die Freiwilligkeit genannt werden:

- Grad der Abhängigkeit,
- Umstände des Einzelfalls,
- rechtliche oder wirtschaftliche Vorteile,
- gleichgelagerte Interessen.

Bei den Umständen des Einzelfalls sollten neben der Art der betroffenen Daten und der Eingriffstiefe auch der Zeitpunkt der Einwilligungserteilung bedacht werden.[865] So nennt die Gesetzesbegründung als Beispiel größerer Drucksituationen die Zeit vor Abschluss eines Arbeitsvertrags.[866]

Als Fälle eines rechtlichen oder wirtschaftlichen Vorteils zählt der Gesetzgeber ein betriebliches Gesundheitsmanagement zur Gesundheitsförderung oder der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen auf.[867] Gleichgelagerte Interessen lägen bei einer Geburtstagliste oder Nutzung von Fotos im Intranet zur Umsetzung eines „betrieblichen Miteinanders“ vor.[868]

8.4.1.2 Formelle Voraussetzungen

Die Einwilligung wurde zunächst unter den Grundsatz des Schriftformerfordernisses gestellt (Abweichungen möglich). Umstritten war, ob hierin ein Verstoß gegen die DSGVO liegt, da zusätzliche Kriterien gegenüber der Einwilligung nach EU-Recht aufgestellt wurden.[869] Zudem wurde kritisiert, dass damit digitale Einwilligungsmanagementlösungen verhindert werden.[870] Entsprechend der Zielsetzung alle Gesetze auf Digitaltauglichkeit zu überprüfen, wurde mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz die elektronische Form hinzugefügt.[871]

---

[864] *Artikel-29-Datenschutzgruppe*, Opinion 2/2017 on data processing at work - WP 249, S. 23.; dagegen grundsätzlich anerkannt: BAG, Urteil vom 11. 12. 2014 – 8 AZR 1010/13, NJW 2015, 2140.
[865] BT-Drs. 18/11325, S. 97.
[866] BT-Drs. 18/11325, S. 97.
[867] BT-Drs. 18/11325, S. 97.
[868] BT-Drs. 18/11325, S. 97.
[869] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 73.
[870] *Brecht u. a.*, PinG 2018, 10 (13).
[871] BT-Drs, 19/11181, S. 19.

§ 26 Abs. 2 S. 3, 4 BDSG

Die Einwilligung hat **schriftlich** oder **elektronisch** zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht […] **in Textform** aufzuklären.

Die DSK fordert in ihrer Entschließung zum Beschäftigtendatenschutz die Formulierung von Regelbeispielen bzw. Bedingungen, in welchen Fällen Einwilligungen im Beschäftigungs- bzw. Bewerbungsverhältnis unzulässig sein sollten.[872]

Praxistipp

Die für die Umsetzung eines KI-Systems erforderlichen Funktionen sollten nicht von der Erteilung einer wirksamen Einwilligung der Beschäftigten abhängig sein, denn:

- Im Beschäftigungskontext verbleiben Zweifel an der Wirksamkeit der Einwilligung aufgrund von Freiwilligkeitsdefiziten.
- Die Einwilligung muss ohne Nachteile jederzeit widerrufbar sein.

Einwilligungen kommen aber dort in Betracht, wo eine Datenbereitstellung optional ist und die Datenbereitstellung auch den Beschäftigten zu Gute kommt.

8.4.2 Generalklausel in § 26 Abs. 1 BDSG

Der deutsche Gesetzgeber hat von der Öffnungsklausel Gebrauch gemacht und den Beschäftigtendatenschutz in § 26 BDSG geregelt. Diese Generalklausel führt die bisherige Regelung vor der DSGVO fort.[873]

§ 26 Abs. 1 S. 1 BDSG

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die

- ▷ Entscheidung über die **Begründung** eines Beschäftigungsverhältnisses oder
- ▷ nach Begründung des Beschäftigungsverhältnisses für dessen **Durchführung** oder
- ▷ **Beendigung** oder

- ▷ zur Ausübung oder Erfüllung der sich aus einem **Gesetz** oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der **Interessenvertretung** der Beschäftigten erforderlich ist.

Der Gesetzgeber hat sich zunächst gegen eine konkretisierende Detailregelung entschieden, aber „behält sich vor“ spezifische Fragen des Datenschutzes im Beschäftigungsverhältnisses entweder im Rahmen dieser Regelung oder eines gesonderten Gesetzes konkretisierend zu regulieren und sich hierbei an der bereits zur

[872] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20220429-Besch%C3%A4ftigtendatenschutz.pdf?__blob=publicationFile&v=1 [letzter Abruf am 30.05.2022], S. 3.

[873] *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 9; *Dietrich u. a.*, DuD 2021, 5 (8).

Vorgängerregelung ergangenen Rechtsprechung zu orientieren.[874] Dies gilt für Problemfelder wie „insbesondere für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken."[875]

Zudem gewährt § 26 Abs. 1 S. 2 BDSG spezifische Orientierung für Arbeitgeber*innen im Hinblick auf den Umgang mit potentiell straffällig gewordenen Beschäftigten:

> **§ 26 Abs. 1 S. 2 BDSG** Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist in § 26 Abs. 3 BDSG geregelt. Daraus ergeben sich insgesamt 3 Erlaubnistatbestände:

- Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (Generalklausel), § 26 Abs. 1 S. 1 BDSG
- Datenverarbeitung zum Zweck der Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG
- Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigtenverhältnis, § 26 Abs. 3 BDSG

Für die Nutzung von Kommunikations- und Kollaborationswerkzeugen im Unternehmen ist der erste Erlaubnistatbestand der relevanteste Ausgangspunkt. Für die aktuelle Regelung sind besonders die folgenden Prüfpunkte maßgeblich, welche im Anschluss besprochen werden sollen:

- Personenbezogene Daten von Beschäftigten (Definition des/der Beschäftigten)
- Zwecke des Beschäftigungsverhältnisses
- Erforderlichkeit

Flankiert werden diese grundlegenden Weichenstellungen mit einem Hinweis auf die Datenschutzgrundprinzipien: § 26 Abs. 5 BDSG enthält einen deklaratorischen Verweis auf die Grundsätze des Art. 5 DSGVO.[876]

Eine Besonderheit der Norm liegt im sachlichen Anwendungsbereich, welcher weiter gefasst ist: § 26 Abs. 7 BDSG legt fest, dass die Regelungen dieses Paragraphen im Beschäftigungsverhältnis auch dann gelten sollen, wenn personenbezogene Daten von Beschäftigten nicht-automatisiert verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[877] § 26 BDSG weicht damit in seinem sachlichen Anwendungsbereich von dem der DSGVO in Art. 2 Abs. 1 DS-GVO (auch bei privaten Stellen) ab, indem die Regelungen für *jegliche* Art der Verarbeitung von Beschäftigtendaten für Gültig erklärt werden.[878] Wie weit diese Ausdehnung reicht, ist wiederum nicht unumstritten. So sollten persönliche und dem „gesellschaftlichen Smalltalk zuzurechnende, nicht protokollierte Gespräche" zwischen Beschäftigten

[874] BT-Drs. 18/11325, S. 97.
[875] BT-Drs. 18/11325, S. 97.
[876] *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 10.
[877] BT-Drs. 18/11325, S. 99.
[878] *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 11; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 29.

und/oder Vorgesetzen nicht unter die datenschutzrechtliche Reglementierung fallen.[879] Bei der Nutzung von KI-Systemen und ähnlichen Kommunikationstools liegt allerdings ohnehin eine automatisierte Datenverarbeitung vor.

8.4.2.1 Zwecke des Beschäftigungsverhältnisses

Hierunter fallen jegliche Zwecke des Beschäftigungsverhältnisses. Diese können sich aus dem Arbeitsvertrag, gesetzlichen Vorschriften (wie z.B. dem Steuerrecht, Sozialversicherungsrecht, etc.) oder Kollektivverträgen ergeben.[880] Unter Kollektivvereinbarungen sind Tarifverträge, Betriebsvereinbarungen und Dienstvereinbarungen zu verstehen (vgl. ErwGr.155 DSGVO).[881] Der Zweck sollte zudem von der Rechtsprechung gebilligt sein. [882]

8.4.2.2 Erforderlichkeit

Zentraler Maßstab der rechtfertigenden Wirkung des § 26 BDSG ist die Frage der *Erforderlichkeit* zur Zweckerreichung.[883] Insbesondere an dieser Stelle gebietet sich ein Rückgriff auf die Grundrechte – denn in Ausfüllung dieser Frage sind die widerstreitenden Grundrechtspositionen in Form der praktischen Konkordanz abzuwägen.[884] „Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.“[885] Da das Kriterium gegenüber der alten Rechtslage vor der DSGVO bewusst beigehalten wurde, kann auf die bisher bereits ergangene Rechtsprechung rekurriert werden.[886]

Das allgemeine Persönlichkeitsrecht schützt die Beschäftigten u.a. vor einer lückenlosen technischen Überwachung am Arbeitsplatz durch heimliche Videoaufnahmen (Totalüberwachung).[887] Eingriffe liegen vor bei Maßnahmen, die einen ständigen Überwachungsdruck erzeugen, dem sich die Beschäftigten während ihrer Tätigkeit nicht entziehen können.[888]

[879] *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 13.
[880] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 24.
[881] BT-Drs. 18/11325, S. 97.
[882] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25.; vgl. auch LAG Berlin-Brandenburg, Urteil vom 30.08.2018 – 26 Sa 1151/17, Rn. 79 f.
[883] *Gräber/Nolden,* in: Paal/Pauly - DS-GVO BDSG, § 26 Rn. 13.
[884] BT-Drs. 18/11325, S. 97; *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 5.
[885] BT-Drs. 18/11325, S. 97.
[886] *Gräber/Nolden,* in: Paal/Pauly - DS-GVO BDSG, § 26 Rn. 14; *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 57; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 23; *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 19; *Dietrich u. a.*, DuD 2021, 5 (8).
[887] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 – BAGE 105, 356-365, Rn. 25; *Dietrich u. a.*, DuD 2021, 5 (8).
[888] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 – BAGE 105, 356-365, Rn. 25; BAG, Urteil vom 07. Oktober 1987 – 5 AZR 116/86 –, Rn. 15

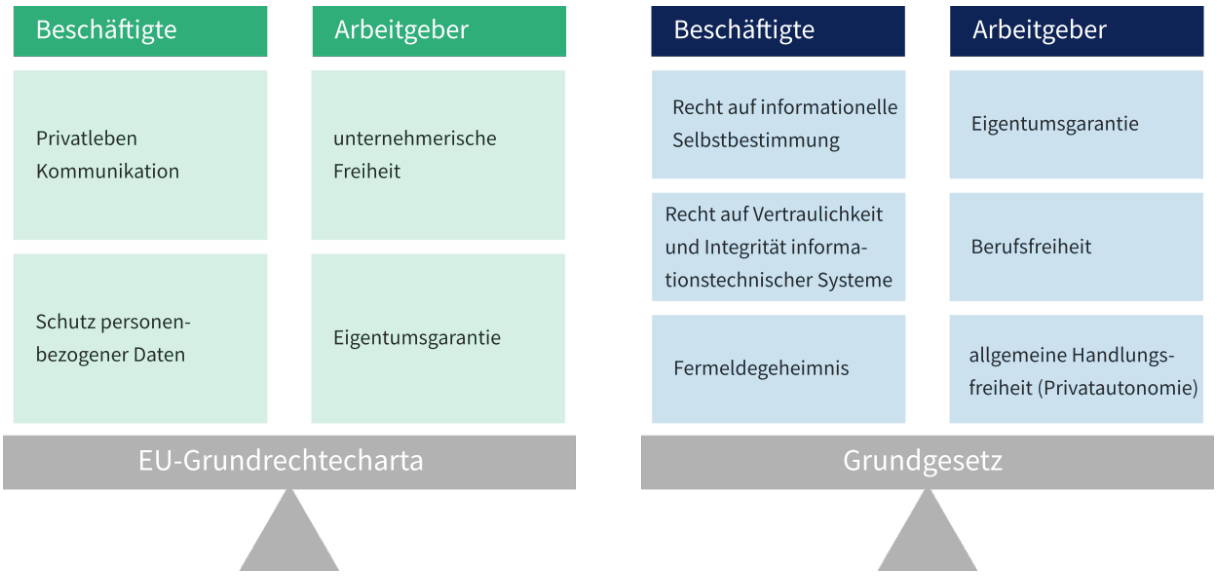


Abbildung 20 Klassische Grundrechtsabwägung im Beschäftigungskontext

Ferner ist Art. 88 Abs. 2 DSGVO als Maßstab heranzuziehen.[889] Zunächst darf also in die Privatsphäre und Persönlichkeitsrechte der Beschäftigten nicht tiefer eingegriffen werden, als dies zur Erfüllung der Zwecke des Beschäftigungsverhältnisses notwendig ist. In Fortführung des bisherigen Systems ist diese Erforderlichkeitsprüfung wie eine Verhältnismäßigkeitsprüfung wie folgt durchzuführen:[890]

Geeignetheit: Im ersten Schritt ist zu prüfen, ob die Maßnahme überhaupt geeignet ist, das verfolgte Ziel zu erreichen oder zumindest zu fördern.[891]

Erforderlichkeit: Im zweiten Schritt ist zu erwägen, ob andere weniger eingriffsintensive Mittel zur Zielerreichung zur Verfügung stehen. [892] Dieses Mittel ist bevorzugt zu nutzen, wenn dieses in gleicher Weise ohne Abstriche bei der Qualität zur Zweckerreichung geeignet ist.[893] Dabei wird Arbeitgeber*innen im Rahmen ihrer Unternehmerfreiheit ein Entscheidungsspielraum über die Organisation betrieblicher Abläufe zugesprochen.[894] Eine existierende grundrechtsschonendere Verarbeitungsmethode muss dann nicht gewählt werden, wenn diese wirtschaftlich nicht zweckmäßig oder technisch gar nicht umsetzbar ist.[895]

Angemessenheit: Im letzten Schritt der Angemessenheitsprüfung erfolgt die Abwägung zwischen den Interessen der Arbeitgeber*innen mit denen der Beschäftigten. Die Schwere des Eingriffs in Arbeitnehmerrechte

[889] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 18; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 23.
[890] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 18; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16; *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 63; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 37.
[891] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16.
[892] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 19; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16.
[893] Vgl. BAG, Beschluss vom 15.04.2014 – 1 ABR 2/13 (B) –, BAGE 148, 26-41, Rn. 41; BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 –, BAGE 105, 356-365, Rn. 32; BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 38; BAG, Urteil vom 22.09.2016 – 2 AZR 848/15 –, BAGE 156, 370-383, Rn. 28; BAG, Urteil vom 20.10.2016 – 2 AZR 395/15 –, BAGE 157, 69-83, Rn. 22; LAG Berlin-Brandenburg, Urteil vom 30.08.2018 - 26 Sa 1151/17, Rn. 80.
[894] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 38.
[895] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 38.

darf nicht außer Verhältnis zum Gewicht der rechtfertigenden Gründe stehen.[896] Hierbei muss ein „unantastbarer Bereich privater Lebensgestaltung in jedem Fall gewahrt bleiben".[897] Zum Teil kann man sich hier an der sog. Sphärentheorie orientieren:[898]

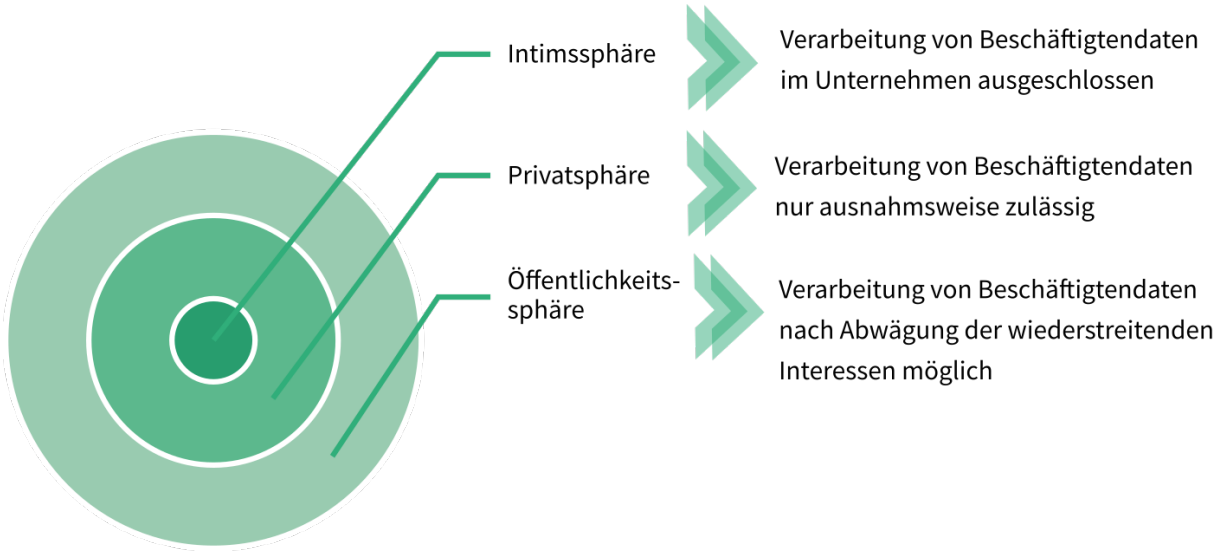


Abbildung 21 Die Sphärentheorie im Beschäftigungskontext

Insgesamt gilt: **Je tiefer der Eingriff in die Persönlichkeitssphäre der Beschäftigten ausfällt, desto gewichtiger müssen die Interessen der Arbeitgeber*innen ausfallen**. Eine „totale, unbegrenzte Überwachung und Erfassung der Daten der Beschäftigten" gilt als unzulässig.[899] Denn dies würde zu einem unzulässigen Überwachungsdruck führen.

Diese Verhältnismäßigkeitsprüfung steht in enger Wechselwirkung zum Grundsatz der Datenminimierung.[900] Denn der Einsatz von Technologien, welche am Ziel ausgereichtet sind so wenig personenbezogene Daten wie möglich zu verarbeiten oder auf Anonymisierung oder Pseudonymisierung setzen, können sich positiv auf die Interessenabwägung auswirken.

Als weiteres Kriterium die Verhältnismäßigkeitsprüfung positiv zu beeinflussen, wird der Grundsatz der Direkterhebung genannt. [901] Hier wird es als weniger Eingriffsintensiv gewertet, wenn Daten bei der betroffenen Person erhoben werden – als wenn diese aus Drittquellen bezogen werden. Auch wenn die DSGVO diesen Grundsatz anders als das BDSG a.F. nicht kennt, dürfte die verbesserte Nachvollziehbarkeit unter dem Aspekt von Treu und Glauben (bzw. Fairness) und Transparenz durchaus auch unter der interpretationsleitenden Maxime der DSGVO weiter beachtet werden können. [902] Denn die betroffene Person erfährt auf diese Weise von der Datenverarbeitung und kann entsprechend ihre Rechte geltend machen.

---

[896] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 19; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 37.; BAG, Urteil vom 17.11.2016 – 2 AZR 730/15 –, Rn. 30; BAG, Beschluss vom 15.04.2014 – 1 ABR 2/13 (B) –, BAGE 148, 26-41, Rn. 41; BAG, Urteil vom 20.06.2013 – 2 AZR 546/12 –, BAGE 145, 278-295, Rn. 23 ff.; BAG, Urteil vom 22.09.2016 – 2 AZR 848/15 –, BAGE 156, 370-383, Rn. 28.

[897] BAG, Urteil vom 7.9.1995 – 8 AZR 828/93, NZA 1996, 637 (638): „Ein unantastbarer Bereich privater Lebensgestaltung muss in jedem Fall gewahrt bleiben"; BAG, Urteil vom 06.06.1984 – 5 AZR 286/81, Rn. 23.

[898] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25.

[899] BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 –, BAGE 111, 173-190, Rn. 44 ff.; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Dietrich u. a.*, DuD 2021, 5 (7).

[900] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 67.

[901] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 68.

[902] Vgl. *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 68.

Ferner können die in ErwGr.47 und 48 DSGVO genannten Kriterien, welche im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO eine Rolle spielen, mit herangezogen werden.[903] Hier sind bspw. die berechtigten Erwartungen der betroffenen Person zu nennen.[904] Insofern bestehen durchaus sich überschneidende Impulse für die Abwägung der Grundrechtskonflikte auf DSGVO- und BDSG-Ebene.

KI-System ist geeignet definierte Anforderungen zu erfüllen	
Ist die Maßnahme überhaupt geeignet, das verfolgte Ziel zu erreichen oder zumindest zu fördern?	– Anforderungsanalyse – Definition der Zielstellungen
Erforderlichkeit eines speziellen KI-Systems	
Existieren andere weniger eingriffsintensive Mittel zur Zielerreichung?	– Überblick über Stand der Technik
Bestehen Abstriche bei der Qualität zur Zweckerreichung?	– Mapping Funktionen mit Zielsetzung
Ist die grundrechtsschonendere Verarbeitungsmethode wirtschaftlich nicht zweckmäßig oder technisch nicht umsetzbar?	– Einschätzung Realisierbarkeit – Abwägung zwischen Risiken und Kosten
Angemessenheit des gewählten KI-Systems	
In welchem Verhältnis steht das Gewicht der rechtfertigenden Gründe zur Schwere des Eingriffs in Arbeitnehmerrechte?	– Risikobewertung – Gesamtabwägung Ziele & Risiken

Tabelle 6 Erforderlichkeitsprüfung nach § 26 Abs. 1 BDSG

8.4.3 Zwischenergebnis zum Beschäftigtendatenschutz und Bedeutung für die KI-Systemnutzung im Unternehmenskontext

Grundsätzlich bestehen verschiedene Möglichkeiten die Verarbeitung personenbezogener Beschäftigtendaten zu legitimieren. Die wesentlichen Herausforderungen sind:

Einwilligung, § 26 Abs. 2 BDSG
Wirksamkeit: Bedenken bestehen insbesondere im Hinblick auf die Freiwilligkeit im Rahmen eines Abhängigkeitsverhältnisses: – Haben die Beschäftigten einen Vorteil von der Datenverarbeitung? – Bestehen gleichlaufende Interessen? **Form:** schriftlich oder elektronisch (außer: andere Form wegen besonderer Umstände angemessen) **Wirkung:** Arbeitgeber*innen sollten zudem Bedenken, dass Einwilligungen jederzeit widerrufbar sind. Im Hinblick auf eine nachhaltige Einführung von KI-basierten Verarbeitungsvorgängen, sollten Einwilligungen auf optional benötigte Daten, auf die nach Widerruf verzichtet werden kann, beschränkt werden.
Verhältnismäßigkeitsprüfung, § 26 Abs. 1 BDSG

[903] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 41.
[904] Siehe Abschnitt 2.4.1.2.4.

Im Rahmen des Beschäftigungskontextes sowie der Erfüllung rechtlicher Verpflichtungen durch die Arbeitgeber*innen richtet sich die Rechtmäßigkeit der Verarbeitung aufgrund des partiellen Richtliniencharakters der DSGVO nicht nach dieser, sondern nach nationalem Recht. Die wichtigste Rechtsgrundlage bietet hier § 26 BDSG, dessen sachlicher und persönlicher Anwendungsbereich weit gezogen wurden. Die Norm ist beim Einsatz von KI-Systemen im Unternehmenskontext relevant, wenn folgende Fragen zutreffen:

- Handelt es sich bei den betroffenen Personen um **Beschäftigte**?
- Erfolgt die Datenverarbeitung für **Zwecke des Beschäftigungsverhältnisses**?
- Ist die Datenverarbeitung erforderlich, d.h. **geeignet, erforderlich und angemessen**?

Betriebsvereinbarung, § 26 Abs. 4 BDSG

Als dritte Option kann die Mitwirkung des Betriebsrats zum Abschluss einer Betriebsvereinbarung Rechtssicherheit schaffen, denn Betriebsvereinbarungen sind eine taugliche Legitimationsgrundlage.[905] Die Wirksamkeit einer Betriebsvereinbarung erfordert die Einhaltung des Verhältnismäßigkeitsgrundsatz. Insofern ist es auch im Rahmen einer Betriebsvereinbarung von Relevanz, ob es sich um datenschutzfreundliche oder datenintensive Lösungen handelt.

8.5 Datenschutzgrundsätze im Beschäftigungskontext

8.5.1 Verweis auf Art. 5 DSGVO

§ 26 Abs. 5 DSGVO verpflichtet den Verantwortlichen explizit geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass insbesondere die in Art. 5 DSGVO dargelegten Grundsätze eingehalten werden.

8.5.2 Datenminimierung im Rahmen des Beschäftigungsverhältnisses

§ 26 Abs. 3 S. 3 i.V.m. § 22 Abs. 2 S. 2 BDSG zählen beispielhaft Schutzmaßnahmen auf, die bei der Verarbeitung *besonderer Kategorien* personenbezogener Daten zu berücksichtigen sind.

1. **technisch organisatorische Maßnahmen (TOMs)**,
2. **Kontrolle & Revisionsfähigkeit:** Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. **Lehrgänge/Schulungen:** Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines **Datenschutzbeauftragten**,
5. **Zugangsbeschränkungen:** Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. **Pseudonymisierung**,
7. **Verschlüsselung**,
8. **Anforderungen an Datenverarbeitungssysteme:** Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Ver-

[905] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 87; *Schrey u. a.*, MMR 2017, 736 (739). Zudem könnte eine ggf. entstandene betriebliche Übung beseitigt werden: *Schrey u. a.*, MMR 2017, 736 (740).

arbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

9. **Interne/externe Audits:** Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs
10. **spezifische Verfahrensregelungen** bei Weiterverarbeitung für andere Zwecke

Diese Maßnahmen zeigen starke Überschneidungen mit Art. 25, 32 DSGVO.[906]

8.5.3 Datenschutz-Folgenabschätzung

In Abschnitt 5.4.4 wurde dargestellt, wann die Pflicht zur Durchführung einer DSFA gegeben ist. Hierfür wurden Kriterien der Artikel-29-Datenschutzgruppe[907] sowie die Positiv-/Negativliste der DSK genannt. Im Beschäftigten- bzw. Unternehmenskontext sind bspw. folgende Punkte dieser Liste besonders hervorzuheben:

Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	– Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen – Geolokalisierung von Beschäftigten	– Zentrale Aufzeichnung der Aktivitäten (z.B. Internetverkehr, Mailverkehr […]) am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. – Ein Unternehmen lässt Bewegungsprofile von Beschäftigen erstellen […].
Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen […] sofern: – Verarbeitung in großem Umfang – für Zwecke, für welche nicht alle Daten direkt bei Betroffenen erhoben – Anwendung von Algorithmen, die für Betroffenen nicht nachvollziehbar – der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	– Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden	Ein Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person	– Kundensupport mittels künstlicher Intelligenz	– Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus – Ein Unternehmen setzt ein System zur Konversation mit Kunden ein, welches für deren Beratung personenbezogene Daten mittels KI verarbeitet

[906] Zur Auslegung siehe: *Rose,* in: Taeger/Gabel - DSGVO/BDSG, § 22 Rn. 51 ff.; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG, § 22 Rn. 12 ff.; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG, § 22 Rn. 33 ff.

[907] *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" - WP248 Rev.01, S. 12.

Tabelle 7 Auszug aus Liste der DSK zu Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist[908]

Beim Einsatz von KI-Systemen im Unternehmen liegen bezüglich der Kriterien der Artikel-29-Datenschutzgruppe der Faktor Machtungleichgewicht und innovative Anwendung neuer Lösungen (zumindest für den Unternehmenskontext) vor. Oftmals wird übersehen, dass über anfallende Metadaten mit Bezug zu Beschäftigten eine Leistungskontrolle möglich ist.[909] Ob hiermit bereits die Schwellen der DSK-Liste erreichen, bedarf einer Betrachtung im Einzelfall. Unternehmen können sich dabei auch einer Einteilung der betroffenen Daten in Schutzklassen bedienen (vgl. Abschnitt 5.4.2.5.3). Es ist daher nicht ausgeschlossen, dass eine DSFA erforderlich werden könnte. Besteht hingegen durch die bereits implementierte technische Gestaltung ein geringes Risiko, bedarf es keiner DSFA.

8.6 Kollektivrechtliche Dimension

Betriebsräte nehmen eine zentrale Rolle ein, da sie die betriebsverfassungsrechtliche Aufgabe wahrnehmen, die Rechte der Beschäftigten zu schützen und zu fördern.[910] Entscheiden sich Unternehmen für den Einsatz von KI-Systemen, müssen zwingend die Mitbestimmungsrechte des Betriebsrats berücksichtigt werden. Diese sind in § 87 BetrVG geregelt. Im Hinblick auf die Digitalisierung im potenziellen Konflikt mit den Arbeitnehmerpersönlichkeitsrechten sind die Abfassung von Verhaltensregeln sowie die Einführung von technischen Systemen, die die Überwachung der Beschäftigten ermöglichen, von besonderer Relevanz und sollen im Folgenden erläutert werden.

8.6.1 Die Rolle des Betriebsrats

Von Arbeitgeberseite ist die Einhaltung der Datenschutzvorschriften aus §§ 75, 80 Betriebsverfassungsgesetz (BetrVG) und auch die Informations- und Mitbestimmungsrechte des Betriebsrats zu beachten. Der Betriebsrat ist die gewählte Arbeitnehmervertretung. Gründungsvoraussetzung sind mindestens fünf ständig, wahlberechtigte Beschäftigte (und drei wählbare Beschäftigte). Den Betriebsrat trifft ebenfalls die Verantwortlichkeit für die Einhaltung der Vorschriften über den Datenschutz.[911]

8.6.2 Mitbestimmungs-, Informations- und Beratungsrechte

Der Aspekt der Künstlichen Intelligenz wurde jüngst klarstellend bezüglich der Unterrichtungs- und Beratungsrechte des Betriebsrats über die Planung von Arbeitsverfahren und Arbeitsabläufen in § 90 BetrVG sowie bezüglich der Mitbestimmung bei Auswahlrichtlinien in § 95 BetrVG aufgenommen. Somit wird sichergestellt, dass die Pflichten der Arbeitgeber*innen und Rechte des Betriebsrats weiterhin gelten, auch wenn KI zum Einsatz kommt.[912] Damit der Betriebsrat seine Beratungs- und Mitbestimmungsrechte tatsächlich wahrnehmen kann, sollte die Einbindung rechtzeitig vor einem geplanten KI-Einsatz erfolgen sowie Unterlagen

908 DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, abrufbar unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf [letzter Abruf 21.07.2021].
909 *Schiering u. a.*, DuD 2020, 161 (162).
910 *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 9.
911 LAG Baden-Württemberg, Beschluss vom 20.05.2022 – 12 TaBV 4/21.
912 *Frank/Heine*, NZA 2021, 1448; *Reinartz*, NZA-RR 2021, 457.

zur Funktionsweise umfassen.[913] Muss der Betriebsrat zur Durchführung seiner Aufgaben die Einführung oder Anwendung von Künstlicher Intelligenz beurteilen, gilt insoweit die Hinzuziehung eines Sachverständigen als erforderlich. Eine Definition des Begriffs „Künstliche Intelligenz“ enthält das BetrVG allerdings nicht.[914]

8.6.2.1 Informationsrechte des Betriebsrats

Der Betriebsrat hat gemäß § 80 Abs. 1 Nr. 1 BetrVG zu überwachen, dass die Vorschriften der DSGVO und des BDSG eingehalten werden, woraus sich für den Betriebsrat aus § 80 Abs. 2 BetrVG ein allgemeiner Informationsanspruch ergibt. Darauf ist bei einer Einführung oder Änderung einer KI und bei der Verarbeitung personenbezogener Daten von Beschäftigten zu achten.[915]Stellt der Betriebsrat ein Auskunftsbegehren nach § 80 Abs. 2 S. 1 BetrVG sind mittels eines Schutzkonzepts die ausreichende Gewährleistung angemessener und spezifischer Schutzmaßnahmen darzulegen, jedenfalls soweit sensitive Daten im Sinne des Art. 9 Abs. 1 DSGVO betroffen sind.[916] Entsprechende Einzelmaßnahmen unterliegen einem Spielraum des Betriebsrates.[917]

8.6.2.2 Mitbestimmungsrechte des Betriebsrats

Für den Einsatz von KI-Systemen im Unternehmen relevante Mitbestimmungsrechte finden sich in:

- § 87 Abs. 1 BetrVG bei der Implementierung eines KI-Systems, das bestimmte Aspekte der Arbeitsorganisation / Arbeitsverhaltens tangiert.
- § 94 BetrVG bei Personalfragebögen und Beurteilungsgrundsätzen in Verbindung mit einem KI-System
- § 95 Abs. 2a BetrVG bei Auswahlrichtlinien auch wenn „Künstliche Intelligenz zum Einsatz kommt“.

Überschneidungen zu datenschutzrechtlichen Fragen bestehen vor allem bei Systemen, die geeignet sind das Verhalten oder die Leistung der Beschäftigten zu überwachen und die Etablierung von Verhaltensregeln bezüglich der Nutzung von IT-Systemen.

8.6.2.2.1 Verhaltensregeln

Nach der Rechtsprechung des Bundesarbeitsgerichts (BAG) greift auch im Rahmen unverbindlicher Verhaltensregeln (wie bspw. einem „Code of Conduct“ oder Ethik-Richtlinien) das Mitbestimmungsrecht aus § 87 Abs. 1 BetrVG, wenn die Maßnahme des Arbeitgebers darauf gerichtet ist, das Verhalten der Beschäftigten zu steuern oder die Ordnung des Betriebs zu gewährleisten.[918] § 87 Abs. 1 Nr. 1 BetrVG berechtigt die Betriebsparteien hingegen nicht, in die private Lebensführung der Beschäftigten einzugreifen. Regelungen über private Beziehungen im Betrieb sind aber nicht von vornherein der Mitbestimmung entzogen.[919] „Betrieb“ ist insofern nicht räumlich, sondern funktional zu verstehen.[920] Daher kann das Mitbestimmungsrecht auch

[913] *Frank/Heine*, NZA 2021, 1448.
[914] *Frank/Heine*, NZA 2021, 1448; *Reinartz*, NZA-RR 2021, 457.
[915] *Raif* in Kramer, IT-Arbeitsrecht, C., Rn. 14.
[916] LAG Baden-Württemberg, Beschluss vom 20.05.2022 – 12 TaBV 4/21.
[917] LAG Baden-Württemberg, Beschluss vom 20.05.2022 – 12 TaBV 4/21.
[918] BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07, Rn. 57 ff.
[919] BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07, Rn. 58 m.w.N.
[920] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03.

dann bestehen, wenn es um das Verhalten der Beschäftigte außerhalb der Betriebsstätte, wie bspw. gegenüber Kundschaft und Lieferanten, geht.[921]

8.6.2.2.2 Mitbestimmungsrechte des Betriebsrats bei Überwachungssystemen

Bei Einsatz technischer Systeme, die eine Überwachung der Arbeitnehmer ermöglichen, ist ebenfalls der Betriebsrat vorab einzuschalten (§ 87 Abs. 1 Nr. 6 BetrVG).[922] Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG wird allerdings erst ausgelöst, wenn eine Leistungs- oder Verhaltenskontrolle durch eine technische Einrichtung ermöglicht wird.[923]

- **„Überwachung“** i.S.d. § 87 Abs.1 Nr. 6 BetrVG ist ein Vorgang, durch den Informationen über das Verhalten oder die Leistung der Arbeitnehmer*in erhoben und so aufgezeichnet werden, dass sie zumindest für eine gewisse Dauer verfügbar bleiben, um sie auch späterer Wahrnehmung zugänglich zu machen.[924] Dabei muss die Überwachung durch die technische Einrichtung selbst bewirkt werden, indem sie auf Grund ihrer technischen Natur unmittelbar, d.h. wenigstens in ihrem Kern das Verhalten oder die Leistung der Beschäftigten kontrolliert.[925] Dabei ist ausreichend, dass die technische Einrichtung zumindest einen Teil des Überwachungsvorgangs ausführt, sofern sie selbst und automatisch die Daten über bestimmte Vorgänge verarbeitet.[926]
- Zur Überwachung **„bestimmt“** sind technische Einrichtungen dann, wenn sie objektiv geeignet sind, Verhaltens- oder Leistungsinformationen der Beschäftigten zu erheben und aufzuzeichnen.[927] Hierbei kommt es auf eine subjektive Überwachungsabsicht des Arbeitgebers nicht an.[928]
- Ein technisches Überwachungssystem gilt auch dann durch die Arbeitgeber*innen als **„angewendet“**, wenn sie bloß im Einvernehmen mit einem Dritten die Beschäftigten anweisen, sich der Überwachung durch dessen technische Einrichtung zu unterwerfen – selbst wenn diese Überwachung in erster Linie oder gar ausschließlich im Interesse des Dritten erfolgt und der:die Arbeitgeber*in keinen Zugriff auf die erfassten Daten nehmen kann.[929] Arbeitgeber*innen sind verpflichtet durch entsprechende Vertragsgestaltung mit dem Dritten sicherzustellen, dass der Betriebsrat sein Mitbestimmungsrecht ausüben kann.[930]

Ob die Einführung und Nutzung eines KI-Systems das Mitbestimmungsrecht des Betriebsrats auslöst, hängt also entscheidend davon ab, ob mit diesem Werkzeug Daten mit Leistungs- bzw. Verhaltensbezug zu den Beschäftigten aufgezeichnet werden und somit eine Kontrollmöglichkeit entsteht – unabhängig davon, ob der Arbeitgeber diese Option tatsächlich zur Überwachung nutzen will. Hintergrund dieses Mitbestimmungsrechts ist die Gefährdung des Persönlichkeitsrechts der Beschäftigten durch eine technisierte Ermittlung von Verhaltens- und Leistungsdaten, wobei auf diese Weise praktisch ununterbrochen und für die betroffenen Personen oft nicht wahrnehmbar und damit weniger durchschaubar eine ungleich größere Anzahl von Daten

[921] BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07, Rn. 58; BAGE 109, 235, Beschluss vom 27.01.2004 - 1 ABR 7/03.
[922] *Fitting,* in: Betriebsverfassungsgesetz, § 87 Rn. 225; *Weisser/Färber*, MMR 2015, 506 (509).
[923] BAG, Beschluss vom 08.11.1994 - 1 ABR 20/94; BAGE 51, 143, Beschluss vom 18.2.1986 - 1 ABR 21/84; BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20 ff.
[924] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20; BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03, Rn. 27.
[925] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20; BAG, Beschluss vom 08.11.1994 – 1 ABR 20/94.
[926] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20.
[927] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03; BAG, Beschluss vom 06.12.1983 - 1 ABR 43/81, NJW 1984, 1476 (1483 f.).
[928] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03; BAG, NJW 1984, 1476 (1484).
[929] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03.
[930] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03 m.w.N.

erhoben werden kann als bei der Überwachung durch Menschen.[931] Technische Kontrolleinrichtungen können in Bereiche eindringen, die einer menschlichen Überwachung nicht zugänglich sind und so die Beschäftigten zum Objekt einer Überwachungstechnik machen, der sie sich nicht entziehen können, sodass diese Technologien nur bei gleichberechtigte Mitbestimmung des Betriebsrats zugelassen werden sollen.[932] Allein **das Wissen darum, dass man zum Objekt einer Überwachungstechnik gemacht wird, kann zu erhöhter Abhängigkeit führen und damit die freie Entfaltung der eigenen Persönlichkeit hindern**.[933]

Auch ist darauf hinzuweisen, dass sich der Arbeitgeber der Mitbestimmungspflicht nicht mit dem Argument entziehen kann, ihm seien Verhaltensregeln oder technische Überwachungseinrichtungen von einem Vertragspartner vorgegeben. Vielmehr liegt es in seinem Verantwortungsbereich bspw. über entsprechende Vertragsgestaltung sicherzustellen, dass die ordnungsgemäße Wahrnehmung der Mitbestimmungsrechte des Betriebsrats gewährleistet ist.[934] Sind anfallende Daten einzelnen Beschäftigten nicht zuordenbar (bspw. bei Verwendung einer nicht individualisierten Zugangskennung), kann bei **Aufzeichnung der Gesamtleistung einer Gruppe ausnahmsweise eine dem Mitbestimmungsrecht unterliegende Einrichtung vorliegen, wenn der auf die Gruppe ausgeübte Überwachungsdruck auf die einzelnen Gruppenmitglieder durchschlägt**. [935]

Beispiele

- Videoüberwachung, Installation von Kameras zur Überwachung des dienstlichen Verhaltens,[936]
- biometrische Zugangskontrolle (Fingerabdruckerfassung),[937]
- Datenverarbeitungssystem zur Evaluation von Trainings- und Weiterqualifizierungsmaßnahmen,[938]
- Arbeitgeberseitig betriebene Facebookseite, die Postings zum Verhalten und zur Leistung der Beschäftigten ermöglicht[939]
- Einrichtung eines Twitter-Accounts[940]

Bei Verletzung der Mitbestimmungsrechte besteht ein Anspruch auf Unterlassung der mitbestimmungswidrigen Maßnahmen.

8.6.3 Beratungsrechte des Betriebsrats

Relevante Beratungsrechte können sein:

- § 90 BetrVG u.a. Planung von Arbeitsverfahren und Arbeitsabläufen „einschließlich des Einsatzes von Künstlicher Intelligenz“
- § 111 BetrVG Einführung grundlegend neuer Arbeitsmethoden.

[931] BAG, Beschluss vom 08.11.1994 – 1 ABR 20/94.
[932] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 27; BAGE 51, 143, Beschluss vom 18.2.1986 - 1 ABR 21/84.
[933] BAG, Beschluss vom 08.11.1994 – 1 ABR 20/94.
[934] BAG, Beschluss vom 27. 1. 2004 – 1 ABR 7/03.
[935] BAG, Beschluss vom 13.12.2016 – 1 ABR 7/15, Rn. 27.
[936] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 –, BAGE 105, 356-365, Rn. 36.
[937] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03 –, BAGE 109, 235-243
[938] BAG, Beschluss vom 14.11.2006 – 1 ABR 4/06 –, BAGE 120, 146-161, Rn. 28
[939] BAG, Beschluss vom 13.12.2016 – 1 ABR 7/15, Rn. 33 ff.
[940] LAG Hamburg, Beschl. v. 13.9.2018 – 2 TaBV 5/18, die Entscheidung wurde mit BAG, Beschluss vom 25.02.2020 - 1 ABR 40/18 allerdings wegen fehlender Antragsbefugnis aufgehoben.

8.6.4 Betriebsvereinbarungen als Rechtsgrundlage

Der Betriebsrat kann als Interessenvertretung der Beschäftigten mit dem Arbeitgeber eine Betriebsvereinbarung über die Einführung und Nutzung des KI-Systems vereinbaren. Hierbei sind bestimmte Grenzen (Beispielsweise geltende tarifvertraglich Regelungen, Einbezug von relevanten Personen (Datenschutzbeauftragten)) zu beachten. Eine Betriebsvereinbarung ist laut ErwGr.155 bzw. Art. 88 DSGVO („Kollektivvereinbarungen einschließlich Betriebsvereinbarungen“) eine Legitimationsgrundlage für die Verarbeitung von Beschäftigtendaten (analog siehe § 26 Abs. 1 BDSG).[941]

Soll eine Betriebsvereinbarung über die Nutzung eines KI-Systems abgeschlossen werden, entfaltet der Schutz der Persönlichkeitsrechte der Beschäftigten als höherrangiges Recht Rahmenbedingungen bezüglich der Wirksamkeit dieses Gestaltungsinstruments, welche zu parallelen Erwägungen wie der Abwägung unter § 26 BDSG führen.[942] So stellte das BAG fest, dass der Umstand einer Zustimmung zu einer Überwachungsmaßnahme durch den Betriebsrat allein jedenfalls dann keine legitimierende Wirkung entfalten kann, wenn keine den Eingriff in die Persönlichkeitsrechte rechtfertigenden Tatsachen vorliegen. [943] Eingriffe sind gerechtfertigt, wenn diese einer Abwägung der widerstreitenden Interessen nach dem Grundsatz der Verhältnismäßigkeit standhalten.[944] Betriebsratsvereinbarungen sollen die Grenzen eines rechtlich zulässigen Eingriffs insofern nicht zulasten der Beschäftigten verschieben.[945]

8.6.5 Zwischenergebnisse: Rechte des Betriebsrats bei der Nutzung von KI-Systemen im Unternehmenskontext

Dem Betriebsrat kommt eine wichtige Funktion zum Ausgleich bei potentiellen Interessenkonflikten zwischen Arbeitgeber- und Arbeitnehmerseite zu. Die Aufnahme des Begriffs der „Künstlichen Intelligenz“ im BetrVG hat allerdings bisher nur klarstellende Bedeutung, sodass hierin derzeit noch keine Erweiterung der Beratungs- und Mitbestimmungsrechte erblickt werden kann. Allerdings wird es dem Betriebsrat vereinfacht externe Sachverständige hinzuzuziehen. Inwiefern der Einsatz von KI-Systemen zu einer Erweiterung der Mitbestimmungsrechte unter dem Gesichtspunkt der Überwachungseignung führt, hängt entscheidend von der technischen Gestaltung ab. Mit der Zunahme der Verfügbarkeit von Daten über die Beschäftigten oder Beschäftigungsabläufe, nehmen auch Möglichkeiten der Verhaltens- und Leistungskontrolle zu. Werden Daten hingegen bspw. umgehend gelöscht, der Zugang zu Daten durch ein Rollen- und Berechtigungsmanagement limitiert, Anonymisierungsmethoden oder andere technische und organisatorische Schutzmaßnahmen eingesetzt, kann die Überwachungseignung ausgeschlossen werden.

8.7 Einsatz von KI-Systemen im Beschäftigungskontext

Expert*innen empfehlen, den Einsatz von Künstlicher Intelligenz im Beschäftigtenkontext gesetzlich zu regeln. Bei der geforderten Regelung des Einsatzes algorithmischer Systeme sollte die Schwere und Tiefe der

[941] Vgl. Zur Wirksamkeit: BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 41; BAG, Beschluss vom 26. August 2008 – 1 ABR 16/07 –, BAGE 127, 276-297, Rn. 14 ff.; BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 –, BAGE 111, 173-190, Rn. 13 ff.
[942] Vgl. BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 –, BAGE 111, 173-190, Rn. 13 ff.
[943] BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 41; BAG, Beschluss vom 26. August 2008 – 1 ABR 16/07 –, BAGE 127, 276-297, Rn. 14 ff.
[944] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02; BAG 17.11.2016 - 2 AZR 730/15, Rn. 31; BAG, Beschluss vom 15.04.2014 – 1 ABR 2/13 (B) –, BAGE 148, 26-41, Rn. 41; LAG Berlin-Brandenburg, Urteil vom 30.08.2018 - 26 Sa 1151/17, Rn. 80.
[945] BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 41 m.w.N.

durch KI-Systeme potentiell bedingten Grundrechtseingriffe den Rahmen vorgeben.[946] Je höher das Schädigungspotential (und damit die Kritikalität) eines Systems ist, desto strenger sollten die Anforderungen für den Einsatz gestaltet werden.[947] Eine gesetzliche Normierung sollte aus Sicht der DSK zudem erfassen:

- Korrektur- und Kontrollinstrumente wie Zulassungsverfahren, Vorabprüfungen,
- Antidiskriminierungsvorgaben,
- Transparenzvorgaben sowie
- verbesserte Möglichkeiten der Rechtsdurchsetzung.

Zudem fordern die Expert*innen klare Verbote bei Profilbildung sowie den Ausschluss der Einwilligung als Grundlage für den Einsatz von KI im Beschäftigungskontext.[948]

Aktuell wird in der Interpretationsbedürftigkeit der Generalklausel des § 26 BDSG das Problem gesehen, dass eine klare und rechtssichere Regelung fehlt, die den Beschäftigten ihre Rechtsposition im Hinblick auf den Schutz ihrer Persönlichkeitsrechte bewusst macht und der Arbeitgeberseite deutlich wird, welche datenschutzrechtlichen Verpflichtungen im Einzelfall zu erfüllen sind.[949] Aktuell obliegt die Ausbalancierung der grundrechtlich verbürgten Rechte noch erheblich bei den datenschutzrechtlich Verantwortlichen (i.d.R. Arbeitgeber*innen) sowie der Einzelfallkasuistik der Arbeitsgerichte. Dies sollte aber Sache des Gesetzgebers sein. [950] Für eine Reform entwickelte der der Beirat für den Beschäftigtendatenschutz Leitgedanken eines spezifischen Regelung des Beschäftigtendatenschutzes: [951]

- *Grundsatz der Verhältnismäßigkeit:* Ausgleich der beiderseitigen Grundrechte unter besonderer Beachtung des Schutzes der Menschenwürde der Beschäftigten, wirksamer Grundrechtsschutz und Rechtssicherheit für alle Beteiligten,
- *Technologieneutralität und Technikoffenheit:* aufgrund der Dynamik der technischen Veränderungen,
- *Transparenz:* für betroffene Beschäftigte und Betriebsräte über die von Arbeitgeber*innen im Zusammenhang mit der Verarbeitung von Beschäftigtendaten verwendeten Einrichtungen und Programme,
- *Gewährleistung einer wirksamen Rechtsdurchsetzung*,
- *Weiterentwicklung des Beschäftigtendatenschutzrechts:* Beachtung der Verhältnismäßigkeit.

Bezüglich der Phase des Bewerbungsverfahrens empfehlen die Expert*innen die reichhaltige Fallpraxis zum Datenerhebungs- und insbesondere dem Fragerecht der Arbeitgeber*innen in typisierbare Fallkonstellationen im Gesetzestext zu überführen, um ein bestmögliches Maß an Wirksamkeit, Rechtssicherheit und Einheitlichkeit zu erreichen.[952] Vergleichbares ist für die Phase der Durchführung des Beschäftigungsverhältnis-

[946] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20220429-Besch%C3%A4ftigtendatenschutz.pdf?__blob=publicationFile&v=1 [letzter Abruf 30.05.2022], S. 2.
[947] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, S. 2.
[948] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 202, S. 2.
[949] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 5.
[950] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 6.
[951] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 6.
[952] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 7.

ses kaum leistbar: hier sind die Fallkonstellationen zu divers um sämtliche in konkretisierenden Tatbeständen zu erfassen. Insofern können nur die Abwägungsparameter weiter ausdifferenziert werden, sowie besonders eingriffsintensive Maßnahmen reguliert. So empfiehlt der Beirat verdeckte Maßnahmen nur in Ausnahmefällen als ultima ratio zur Aufdeckung von Straftaten zuzulassen. [953] Zudem sollten Kontrollmechanismen etabliert werden, sodass verdeckte Maßnahmen den Einbezug von betrieblichen oder außerbetrieblichen Akteuren erfordert. Daneben wird gefordert die Einwilligung an das Vorliegen besonderer Umstände zu knüpfen, welche die Freiwilligkeit sicherstellen. Solche Umstände, wie eigene oder gleichgelagerte Interessen seien im Bewerbungsstadium ausgeschlossen.[954]

Zur Regelung des KI-Einsatzes können die sieben datenschutzrechtlichen Anforderungen der Hambacher Erklärung der Datenschutzkonferenz (DSK) Orientierung bieten:[955]

- KI darf Menschen nicht zum Objekt machen
- KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben
- KI muss transparent, nachvollziehbar und erklärbar sein
- KI muss Diskriminierungen vermeiden
- Für KI gilt der Grundsatz der Datenminimierung
- KI braucht Verantwortlichkeit
- KI benötigt technische und organisatorische Standards

Der erste Grundsatz folgt aus dem Schutz der Menschenwürde (vgl. Abschnitt 3.1.1). Zur Umsetzung sollten Betroffene laut DSK den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung haben.[956] Die Transparenz sollte sich auf den Prozess der Verarbeitung als auch die Trainingsdaten beziehen. Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, sollten nachvollziehbar und erklärbar im Hinblick auf das Ergebnis, die Prozesse sowie das Zustandekommen der Entscheidungen sein. [957] Da Diskriminierungsneigungen, aufgrund unzureichender Datengrundlagen oder Konzeption, oftmals nicht offensichtlich sind, sollten Risiken vorab bewertet werden und während der Anwendung eine Risikoüberwachung erfolgen, um auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. [958]

[953] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 7.
[954] *Beirat für den Beschäftigtendatenschutz*, Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, S. 8.
[955] *Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Hambacher Erklärung zur Künstlichen Intelligenz, S. 3 ff.
[956] *Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Hambacher Erklärung zur Künstlichen Intelligenz, S. 3.
[957] *Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Hambacher Erklärung zur Künstlichen Intelligenz, S. 3.
[958] *Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Hambacher Erklärung zur Künstlichen Intelligenz, S. 4.

9 Forschungsdatenschutz

Sonderregelungen zur Forschung finden sich sowohl in der DSGVO, im BDSG als auch in den Landesdatenschutzgesetzen, sodass sich für Forschungsprojekte oftmals zunächst die Frage nach dem einschlägigen Rechtsrahmen stellt. Zudem ist der Begriff der „Forschung“ nicht explizit definiert.

9.1 Definition von Forschung

Es existiert keine universell anerkannte Definition von Forschung oder Wissenschaft.[959] Auf EU-Ebene enthält die Open-Data-Richtlinie eine Definition von Forschungsdaten:

> **Art. 2 Nr. 9 RL (EU) 2019/1024** „Forschungsdaten“ Dokumente in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als **Nachweise** im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden;

Zum Begriff der Forschung wird in Deutschland auf die Rechtsprechung des BVerfG zu Art. 5 Abs. 3 GG rekurriert. Danach ist Forschung ein auf wissenschaftlicher Methodik beruhender systematisch-geistiger und nachprüfbarer Prozess zum Erkenntnisgewinn, Erkenntnisdeutung und Weitergabe.[960] Umfasst ist „alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist“.[961] Art. 3 Nr. 10 DNG definiert Forschungsdaten entsprechend der Open-Data-Richtlinie.[962]

Auch auf europäischer Ebene wird auf systematische Aktivitäten abgestellt, welche die Sammlung und Analyse von Daten einschließen, um den Bestand an Erkenntnissen und Wissen und deren Anwendung zu erweitern.[963] Die EU-Kommission unterstreicht dabei die Zielsetzung der europäischen Wissenschaftspolitik den Innovationsprozess auch für Menschen aus anderen Bereichen als der akademischen und wissenschaftlichen Welt zu „öffnen" und bei der Verbreitung des Wissens zu unterstützen, sobald es unter Verwendung digitaler und kollaborativer Technologien verfügbar ist sowie die internationale Zusammenarbeit in der Forschungsgemeinschaft zu fördern.[964] Der DSGVO liegt ebenfalls ein weites Verständnis zur Forschung zugrunde, das nicht zwischen Forschung durch öffentliche oder private Stellen differenziert.[965] Nach ErwGr 159 soll Forschung die technologische Entwicklung sowie die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Die Artikel-29-Datenschutzgruppe forderte zusätzlich die Einhaltung sektorbezogener methodischer und ethischer Standards um in den Genuss von Forschungsprivilegien im Datenschutzrecht zu kommen.[966] Im Ergebnis sind diese Privilegien also nicht auf Hochschulen oder Forschungseinrichtungen beschränkt, sondern an der Tätigkeit „Forschung“ orientiert.

---

[959] *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research.
[960] BVerfGE 35, 79, 112 f.; 47, 327, 367.
[961] BVerfGE 35, 79, 112.
[962] „Aufzeichnungen in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden.“
[963] *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, S. 9.
[964] *EU-Kommission,* Open innovation, open science, open to the world: A vision for Europe, Mai 2016, S. 31 ff.; *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, S. 9.
[965] *Louven,* in: Taeger/Gabel, BDSG § 27, Rn. 5.
[966] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 28.

9.2 Einschlägiger Rechtsrahmen und Rechtsgrundlagen

	Art der Einrichtung	Rechtsgrundlagen
Öffentliche Stellen	Hochschulen	LDSG (§ 13 LDSG BW) ergänzt durch DSGVO
	Bundeseigene Institutionen	§ 27 BDSG ergänzt durch DSGVO
Nicht-öffentliche Stellen	Außeruniversitäre Einrichtung (privatrechtlich organisiert)	Art. 6 Abs. 1 DSGVO § 27 BDSG (besondere Kategorien)
	Unternehmen	Art. 6 Abs. 1 DSGVO § 27 BDSG (besondere Kategorien)

Tabelle 8 Rechtsgrundlagen in der Forschung

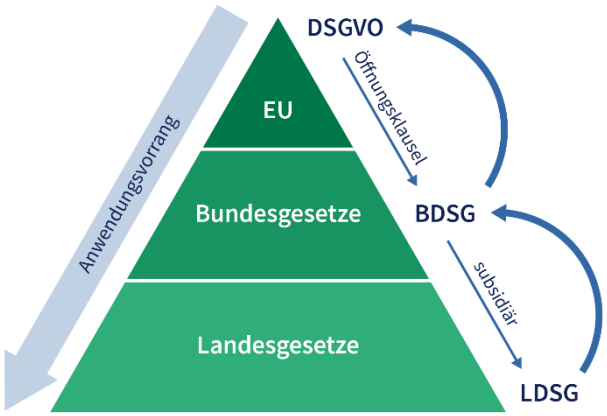


Abbildung 22 Regelungshierarchie

In Baden-Württemberg ist das Landesdatenschutzrecht nach § 2 Abs. 1 S. 1 LDSG anwendbar für **öffentliche Stellen**, wobei es sich um Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts handelt. Hierzu zählen auch Hochschulen. Eine spezielle Forschungsklausel enthält § 13 LDSG BW.

> Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. […].

§ 27 Abs. 1 BDSG regelt die Datenverarbeitung zu Forschungszwecken und zu statistischen Zwecken bezüglich besonderer Kategorien personenbezogener Daten. Absatz 4 bezieht sich hingegen seinem Wortlaut nach wiederum auf „personenbezogene Daten".

Für privatrechtlich organisierte Forschungseinrichtungen sowie Unternehmensforschung gilt hingegen die DSGVO. Die Verarbeitung personenbezogener Daten zu Forschungszwecken kann hier auf die bereits beschriebene Einwilligung oder Interessenabwägung gestützt werden. Auf die Interessenabwägung können sich allerdings Behörden bei Erfüllung ihrer Aufgaben nicht berufen. Sofern man nach einem weiten Verständnis des Begriffs der Behörde („public authorities" in der engl. Sprachfassung) auch Hochschulen dazu zählt,[967] orientiert sich das anwendbare Recht an der Organisationsform der Forschungseinrichtung.

Die Regelungshierarchie (Anwendungsvorrang des EU-Rechts vor mitgliedstaatlichem Recht sowie Bundes- vor Landesrecht) wird beim Forschungsdatenschutz aufgrund von Öffnungsklauseln und Subsidiaritätsregelungen quasi auf den Kopf gestellt (vgl. Abbildung 22).

[967] So *Golla*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23 Datenschutz in Forschung und Hochschullehre, Rn. 45.

9.3 Privilegierungen der Forschung

9.3.1 Privilegierungen im Rahmen der Einwilligung: Broad Consent

Sofern die Einholung von Einwilligungserklärungen im jeweiligen Forschungskontext möglich ist, stellt das Instrument der Einwilligung Rechtssicherheit her und gewährleistet die Selbstbestimmung der Betroffenen.[968] Diese ist nur wirksam, wenn sie spezifisch für *bestimmte Zwecke* erteilt wurde. Pauschaleinwilligungen sind nicht möglich.[969] Da sich im Laufe einer Forschungstätigkeit aufbauend auf neuen Erkenntnissen oftmals neue Forschungszwecke und Forschungsfragen stellen, können diese nicht immer zum Zeitpunkt der Einwilligungseinholung genau beschrieben werden.[970] Dieser Umstand wird in ErwGr. 33 DSGVO aufgegriffen: Bei der Auslegung und Anwendungen der Normen zur Einwilligung sollte daher bedacht werden, dass es betroffenen Personen erlaubt sein sollte, ihre Einwilligung für *bestimmte Bereiche wissenschaftlicher Forschung* zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen. Die Artikel-29-Datenschutzgruppe unterstreicht dabei, dass ErwGr. 33 keine Aufgabe des Grundsatzes der Zweckfestlegung darstellt, dagegen aber bei der Beschreibung mehr Flexibilität bietet.[971] Die DSK präferiert dagegen eine enge Auslegung, wonach „*nur wenn das konkrete Design des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung schlechthin nicht zulässt […], kann beispielsweise der Ansatz der breiten Einwilligung (broad consent) zum Tragen kommen*“.[972]

Bei der Einhaltung wissenschaftlicher Standards sind neben anerkannten ethischen Standards, auch normative und prozessuale Festlegungen sowie technisch-organisatorische Vorkehrungen zu berücksichtigen.[973] Der European Data Protection Supervisor fordert zudem den Mangel der Zweckspezifikation kompensierende Transparenz- und Schutzmaßnahmen.[974] Solche zusätzlichen Transparenzmaßnahmen können einen Mangel der Zweckspezifikation kompensieren, insbesondere wenn Informationen über die Entwicklung der verfolgten Forschungszwecke im Laufe des Forschungsprojekts regelmäßig zur Verfügung gestellt werden.[975]

Empfohlen werden gestufte Optionen mit echten Wahlmöglichkeiten bis hin zum Open Access.[976] Ein Beispiel könnte wie folgt aussehen:

[968] *Golla,* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23 Datenschutz in Forschung und Hochschullehre, Rn. 21.
[969] vgl. *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 29; *Weisser/Färber*, MMR 2015, 506 (509); *vbw - Vereinigung der Bayerischen Wirtschaft e. V.*, Automatisiertes Fahren – Datenschutz und Datensicherheit, S. 18 f.
[970] *Golla,* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23 Datenschutz in Forschung und Hochschullehre, Rn. 22.
[971] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 28.
[972] *DSK - Datenschutzkonferenz*, Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO.
[973] *Weichert*, ZD 2020, 18 (21).
[974] *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research.
[975] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 28.
[976] *Wirth*, ZUM 2020, 585; *Schaar*, ZD 2017, 213; *Gläss/Drepper,* in: Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data, S. 25.

☐ Ich willige in die Verarbeitung personenbezogener Daten durch „ABC“ ein, soweit dies erforderlich für die Durchführung der Studie „XYZ“ ist.

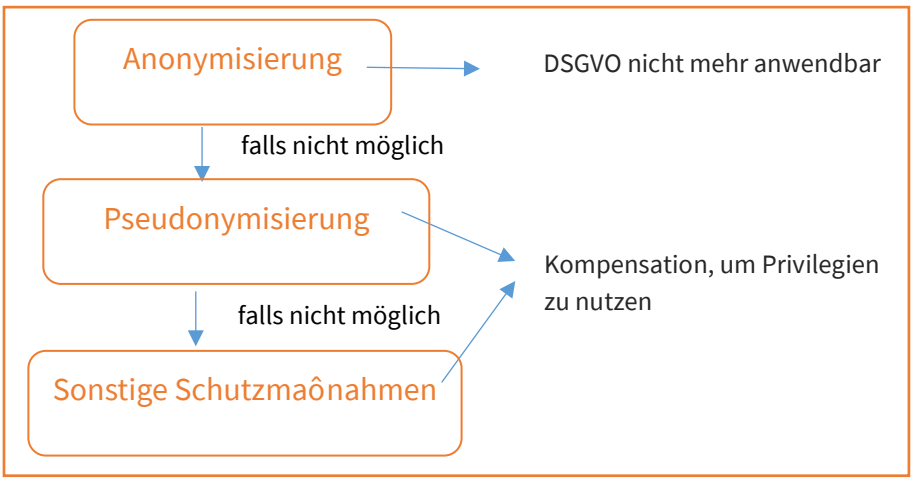
☐ Darüber hinaus willige ich in die Weiternutzung der Daten durch „ABC“ auch nach Abschluss der Studie für Forschung zum Thema „XYZ“ ein.

☐ Darüber hinaus willige ich ein, dass meine personenbezogenen Daten für weitere Forschungsprojekte im Bereich „XYZ“ verwendet werden können. Hierzu dürfen meine Daten mit anderen Forschungseinrichtungen geteilt werden.

9.3.2 Privilegierung im Rahmen der Zweckbindung

Jede Verarbeitung personenbezogener Daten unterliegt grundsätzlich dem Prinzip der Zweckbindung (vgl. Art. 8 Abs. 2 S. 1 GrCh, Art. 5 Abs. 1 Buchst. b) DSGVO), wonach eine Weiterverarbeitung zu anderen Zwecken Grenzen gesetzt sind. Allerdings soll eine Weiterverarbeitung u.a. zu Forschungszwecken nicht als unvereinbar mit den ursprünglichen Zwecken gelten. Umstritten bleibt die Interpretation: nach einer Ansicht greift die „*Fiktion der Zweckidentität*“, wenn die in Art. 89 Abs. 1 DSGVO genannten Garantien eingehalten werden.[977] Andere verlangen weiterhin einen Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO zwischen Primär- und Sekundärnutzung – wenn auch unter der Annahme, dass im „Regelfall“ eine Vereinbarkeit der Zwecke gegeben sei.[978] Art. 5 Abs. 1 Buchst. b DSGVO könnte auch als gesetzliche (widerlegbare) Vermutung gewertet werden.[979] Insofern verbleibt eine Rechtsunsicherheit. Forschende sollten eine ausgewogene Balance zwischen Risiken und diese kompensierenden Transparenz- und Schutzmaßnahmen orientieren.

Art. 89 Abs. 1 DSGVO verlangt für die Privilegierung das Vorliegen von „Garantien“ (Schutzmaßnahmen). Hier steht die Achtung des Grundsatzes der Datenminimierung im Wege der Pseudonymisierung oder Anonymisierung prominent im Vordergrund. Sowohl Art. 89 DSGVO, § 27 Abs. 4 BDSG und bspw. § 13 Abs. 2 LDSG BW enthalten Pflichten zur Anonymisierung bzw. Pseudonymisierung, sobald dies nach dem Forschungszweck möglich ist. Allerdings muss in Zeiten von Big-Data ebenfalls anerkannt werden, dass die faktischen Möglichkeiten der Re-Identifizierung von scheinbar anonymisierten Datensätzen fast unbegrenzt sind.[980]



[977] *Weichert*, ZD 2020, 18 (21).
[978] *Roßnagel*, ZD 2019, 157.
[979] *Monreal*, ZD 2016, 507.
[980] *Weichert*, in: Stiftung Datenschutz, Big Data und E-Health, S. 187.

Ein Überblick über grundsätzlich geeignete Maßnahmen ist in Tabelle 9 zusammengefasst.[981]

Datenminimierung: - Anonymisierung - Pseudonymisierung - Löschfristen	**Nachvollziehbarkeit:** - Protokollierung - Spezifische Verfahrensregelungen bei Übermittlung oder Zweckänderung
Kompetenz: - Sensibilisierung der an der Verarbeitung beteiligten Personen - Benennung bzw. Einbeziehung eines/einer Datenschutzbeauftragten - Einbeziehung einer Ethik-Kommission	**Datensicherheit:** - Verschlüsselung - Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit - Zugangsregelungen - Regelmäßige Überprüfung und Evaluierung

Tabelle 9 Beispiele für geeignete Garantien nach Art. 89 DSGVO

9.3.3 Privilegierung im Rahmen der Speicherbegrenzung

Auch zum Grundsatz der Speicherbegrenzung findet sich eine Aufweichung der datenschutzrechtlichen Anforderungen für die Verfolgung von Forschungszwecken. Bei ernsthafter Beeinträchtigung der Forschungsziele kann eine Löschung unterbleiben, bspw. wenn die Forschung auf die Vollständigkeit der Daten zwingend angewiesen ist. Bei restriktiver Auslegung, wären Forschungsdaten zur Beendigung des Forschungsprojekts zu löschen. Die Erforderlichkeit zur längerfristigen Speicherung könnte auch aus den Leitlinien guter wissenschaftlicher Praxis folgen, die eine Archivierung über 10 Jahre fordern.[982] Diese Speicherung steht ebenfalls unter dem Vorbehalt technisch und organisatorischer Schutzmaßnahmen (vgl. Art. 89 DSGVO).[983]

9.3.4 Privilegierung bei der Herstellung von Transparenz und Betroffenenrechten

Informationspflichten: Sofern Daten nicht bei der betroffenen Person selbst erhoben werden, kann im Forschungskontext eine Information ausnahmsweise bei Unmöglichkeit, unverhältnismäßigem Aufwand oder ernsthafter Beeinträchtigung der Forschungsziele unterbleiben (Art. 14 Abs. 5 DSGVO). Unklarheiten verbleiben, ob Unmöglichkeit bzw. Unverhältnismäßigkeit objektiv oder subjektiv nach den Fähigkeiten des Verantwortlichen zu bestimmen sind und welcher Aufwand noch zumutbar ist.[984] Auch sieht Art. 13 DSGVO keine vergleichbare Ausnahme vor. Wird bspw. die Datenaufzeichnung im öffentlichen Straßenraum als „bei der betroffenen Person erhoben“ bewertet, greift derzeit keine explizite Privilegierung. Dies stellt bspw. die Forschung zum autonomen Fahren vor Herausforderungen, realistisch sicherzustellen, dass selbst bei schnell vorbeifahrenden Fahrzeugen die Informationen wahrnehmbar sind.

Auskunftsrechte: Weitere Regelungen sehen die Einschränkung des Auskunftsrechts vor (§ 27 Abs. 2 BDSG,

[981] Wagner, Das neue Mobilitätsrecht, S. 176, basierend auf: Weichert, ZD 2020, 18 (21).
[982] *Roßnagel*, ZD 2019, 157.
[983] *Wirth*, ZUM 2020, 585.
[984] *Schmidt-Wudy,* in: *Wolff/Brink*, BeckOK DatenschutzR. Art. 14 Rn. 98; *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG. Art. 14 Rn. 40d m.w.N.

§ 13 Abs. 4 LDSG BW). Kritisiert wird diesbezüglich allerdings eine mögliche Überschreitung der Regelungskompetenz sowie das Fehlen konkretisierender Kriterien.[985] Wann ein unverhältnismäßiger Aufwand anzunehmen ist, sollte entsprechend der Regelung des Art. 14 Abs. 5 Buchst. b) DSGVO einheitlich ausgelegt werden.[986] Die Ausnahme könnte zur Anwendung kommen, wenn besonders große Datenbestände ausgewertet werden oder sich Betroffene nur schwer identifizieren lassen.[987]

§ 13 Abs. 4 LDSG BW, § 27 Abs. 2 BDSG	
- Beschränkung der Rechte auf: ▪ Auskunft (Art. 15 DSGVO), ▪ Berichtigung (Art.16 DSGVO), ▪ Einschränkung der Verarbeitung (Art. 18 DSGVO) und ▪ Widerspruch (Art. 21 DSGVO), - soweit diese Rechte voraussichtlich die Verwirklichung der jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und - die Beschränkung für die Erfüllung der jeweiligen Forschungs- oder Statistikzwecke notwendig ist.	Das Recht auf Auskunft gemäß Art. 15 DSGVO besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.
Grundlage: Art. 89 Abs. 2 DSGVO	Keine Grundlage in DSGVO

9.4 Begrenzung bei der Veröffentlichung von Daten

Außer mit Einwilligung dürfen personenbezogene Daten nur veröffentlicht werden, soweit dies für die Darstellung von Forschungsergebnissen *über Ereignisse der Zeitgeschichte unerlässlich* ist. Dies entspricht sowohl der Regelung in § 27 Abs. 4 BDSG als auch § 13 Abs. 3 LDSG BW. Hintergrund der Regelung ist der Umgang mit Forschungsergebnissen.[988] Eine Veröffentlichung liegt vor, wenn die personenbezogenen Daten einem bestimmbaren oder unbestimmbaren Personenkreis zugänglich gemacht werden.[989] Privilegiert wird hier nur die historische Forschung.[990] Die Veröffentlichung unterliegt somit für sonstige Forschungsprojekte dem Einwilligungsvorbehalt.[991] Ist ein Forschungsprojekt dem Open-Access-Gedanken entsprechend nicht nur auf die diskriminierungsfreie Zugänglichkeit der Forschungsergebnisse sondern auch der Forschungsmaterialien und (Roh-)Daten ausgelegt, dürfte dies nur mit Einwilligung oder anonymisierten Daten umsetzbar sein.

[985] *Schaar*, ZD 2017, 213; *Johannes/Richter*, DuD 2017, 300.
[986] *Golla,* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23 Datenschutz in Forschung und Hochschullehre, Rn. 54.
[987] *Krohm,* in: Gola/Heckmann, BDSG § 27, Rn. 38; *Louven,* in: Taeger/Gabel, BDSG § 27, Rn. 15; *Pauly,* in: Paal/Pauly, BDSG § 27, Rn. 13.
[988] LT-Drs. (BW) 16/3930, 101; LT-Drs. (Nds.) 18/548, 51.
[989] *Pauly,* in: Paal/Pauly, BDSG § 27, Rn. 21; *Krohm,* in: Gola/Heckmann, BDSG § 27, Rn. 44.
[990] Pauly, in: Paal/Pauly, BDSG § 27, Rn. 20; *Golla,* in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 23 Datenschutz in Forschung und Hochschullehre, Rn. 30.
[991] *Krohm,* in: Gola/Heckmann, BDSG § 27, Rn. 43.

10 Kontextspezifische Datenschutzanforderungen

Je nach Kontext des KI-Einsatzes existieren weitere datenschutzrechtliche Anforderungen, welche die bereits behandelten Themen entweder ergänzen oder überlagern können. Handelt es sich um besondere Kategorien personenbezogener Daten, gelten weitere Schutzvoraussetzungen zu beachten. Mit der DSGVO sind auch wettbewerbsrechtliche Elemente mit dem Recht auf Datenübertragbarkeit, auch Recht auf Datenportabilität genannt, eingezogen. Dieses Recht ist aber nicht in allen Datenverarbeitungskontexten einschlägig. Besondere Anforderungen stellen sich zudem, wenn es im Rahmen der Nutzung von KI-Systemen zu einem Datentransfer in Drittländer außerhalb der EU bzw. des EWR kommt. Dagegen unterliegt der Datenschutz sowie der Schutz des Fernmeldegeheimnisses spezialrechtlicher Regelungen zur elektronischen Kommunikation.

10.1 Besonders schutzbedürftige Daten

Die unter Abschnitt 6 geschilderten Legitimationsgrundlagen betreffen die Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 DSGVO. Allerdings kennt die DSGVO besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, für deren Verarbeitung weitere Anforderungen gelten.

10.1.1 Verbot der Verarbeitung

Art. 9 Abs. 1 DSGVO besagt zunächst, dass die Verarbeitung folgender Daten verboten ist:

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung.

10.1.2 Ausnahmen vom Verarbeitungsverbot

10.1.2.1 Ausdrückliche Einwilligung

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten, in der ein besonderes Risiko für die Rechte der betroffenen Personen bestehen kann, reicht eine einfache Einwilligung nicht aus, vielmehr muss diese durch eine ausdrückliche Einverständniserklärung ausdrücken, dass sich die betroffene Person dieser Risiken bewusst ist.[992] Somit ist bei der Verarbeitung sensibler Daten ein gesteigertes Maß an Bestimmtheit erforderlich, wozu sowohl ein Hinweis auf die Sensitivität oder besonderen Charakter der Daten als auch die Genauigkeit in Bezug auf die Nennung der konkret betroffenen Daten und des Verwendungszwecks gezählt

[992] *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, S. 19; *Roßnagel*, ZD 2019, 157 (161).

wird.[993] Das Erfordernis der Ausdrücklichkeit ändert zwar grundsätzlich nichts an der generellen Formlosigkeit der Einwilligung.[994] Eine Einwilligung durch schlüssiges oder konkludentes Verhalten wird in der Literatur allerdings ausgeschlossen.[995] Folglich steigern sich die Anforderungen an die Einwilligung sowohl in inhaltlicher Sicht im Hinblick auf Aufklärung und Verständlichkeit als auch in praktischer Sicht bezüglich des Aktivitätslevels bei Erteilung der Einwilligungserklärung.

In § 26 Abs. 3 S. 2 BDSG wird ebenfalls ausgedrückt, dass auch bei der Verarbeitung besonderer Kategorien personenbezogener Daten eine Einwilligung nach den genannten Maßstäben grundsätzlich möglich ist, sich die Einwilligungserklärung allerdings ausdrücklich auf diese Daten beziehen muss.

10.1.2.2 Ausnahmen im Arbeitsrecht

Neben der Einwilligung sieht Art. 9 Abs. 2 DSGVO weitere Möglichkeiten der Ausnahme vom Verarbeitungsverbot vor. Für den KI-Einsatz im Beschäftigungskontext könnten folgende Aspekte relevant werden:

Art. 9 Abs. 2 Buchst. b DSGVO trägt dem Umstand Rechnung, dass Arbeitgeber*innen im Rahmen des Beschäftigungsverhältnisses eine Vielzahl auch unter den Katalog des Art. 9 Abs. 1 DSGVO fallende Daten verarbeiten müssen. Hierbei handelt es sich nicht um einen Legitimationstatbestand selbst, sondern es wird auf das Recht der Union, der Mitgliedstaaten, Betriebsvereinbarungen und Tarifverträge verwiesen.[996] Erfasst wären – sofern spezialgesetzlich verankert – Verarbeitungsbefugnisse bspw. zu Zwecken der Renten- und Sozialversicherung, Krankenversicherung, Krankheitstage, Sozialhilfe, Wohnungs-, Familien- oder Ausbildungsförderung.[997] Entscheidende Hürden sind zum einen das Kriterium der Erforderlichkeit und zum anderen „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ eingerichtet werden.[998] Die Garantien werden nicht definiert, in der Literatur erörtert werden sowohl die Verstärkung der Betroffenenrechte (auf Auskunft, Berichtigung, Löschung etc.) als auch technische und organisatorische Maßnahmen (bspw. Pseudonymisierung und Verschlüsselung).[999] Dies bedeutet aber auch, dass Daten bspw. zum gesundheitlichen Zustand bei Krankmeldungen besonders geschützt in Personalakten verwahrt werden müssen, sodass eine zufällige Kenntnisnahme ausgeschlossen ist. [1000]

Im Rahmen der Sonderregelung zum Beschäftigtendatenschutz im BDSG widmet sich § 26 Abs. 3 BDSG der Verarbeitung besonderer Kategorien personenbezogener Daten. Diese ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Insofern ist auch hier eine Erforderlichkeitsprüfung durchzuführen.[1001] Flankierend sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (vgl. § 22 Abs. 2 BDSG). Je wirkungsvoller die gewählten Schutzmaßnahmen sind, desto eher fällt eine Interessenabwägung zugunsten der Zulässigkeit einer

[993] *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 51; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 47.
[994] *Samardzic/Becker*, EuZW 2020, 646 (651).
[995] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 47; *Molnár-Gábor*, DSRITB 2018, 159 (163).
[996] *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 52; *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 20; *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 21; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 37.
[997] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 20; *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 21.
[998] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 39; für eine enge Auslegung: *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 54; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 41.
[999] *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 28.
[1000] BAG, Urteil vom 12.9.2006 – 9 AZR 271/06, Rn. 22 ff.; *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 40.
[1001] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 51.

Datenverarbeitung aus.[1002]

Rechtsprechung der Arbeitsgerichte

- Personalakten dürfen nicht allgemein zugänglich sein und müssen sorgfältig verwahrt werden (BAG, Urteil vom 12.9.2006 – 9 AZR 271/06):
  - „Das Geheimhaltungserfordernis im Hinblick auf Teile der Personalakte kann durchaus unterschiedlich sein. […] Zu den besonders sensiblen Daten gehören insbesondere solche über den körperlichen, geistigen und gesundheitlichen Zustand und allgemeine Aussagen über die Persönlichkeit des Arbeitnehmers. Sie bedürfen deshalb des verstärkten Schutzes."
  - „Grundsätzlich hat der Arbeitnehmer keinen Anspruch auf eine bestimmte Art und Weise der Geheimniswahrung sensibler Daten. […] Dabei obliegt es grundsätzlich dem Arbeitgeber im Rahmen seiner Personal- und Organisationsfreiheit zu bestimmen, wie das besondere Geheimhaltungsbedürfnis des Arbeitnehmers an sensiblen Daten umgesetzt wird."

10.1.2.3 Offensichtlich öffentlich gemachte Daten

Art. 9 Abs. 2 Buchst. e DSGVO erlaubt die Verarbeitung besonderer Kategorien personenbezogener Daten, wenn es sich um Daten handelt, „die die betroffene Person offensichtlich öffentlich gemacht hat". In diesem Fall besteht keine besondere Schutzbedürftigkeit.[1003] Der Verantwortliche muss in diesem Fall die Rechtmäßigkeit der Verarbeitung aber weiterhin an Art. 6 Abs. 1 DSGVO messen.[1004] Voraussetzungen sind:

- Öffentlichkeit der Daten: ist gegeben, sofern die Daten dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offen stehen.[1005] Bei sozialen Netzwerken ist dies der Fall, wenn die Daten der Allgemeinheit zugänglich sind und nicht nur innerhalb geschlossener/privater Gruppen geteilt wurden.[1006] Abgrenzungsschwierigkeiten bestehen bei Gruppen, die aus einer nicht mehr eindeutig bestimmbaren Personengruppe bestehen bzw. bei denen alle Interessierten Mitglied werden können.[1007]
- Offensichtliche Veröffentlichung durch betroffene Person selbst: die Veranlassung muss sichtbar von der betroffenen Person selbst erfolgt sein, selbst wenn diese (bspw. im Rahmen der Presseberichterstattung) von Dritten durchgeführt wird. [1008] Es muss aus Sicht eines objektiven Dritten ein unzweideutiger, bewusster Willensakt, der final auf die Entäußerung der Information gerichtet ist, gegeben

[1002] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 53.
[1003] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 25.
[1004] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 77; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 64; *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 25; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 57.
[1005] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 26; *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 45; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 78; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 65.
[1006] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 26.
[1007] vgl. auch *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 58.
[1008] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 79; *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 26.

sein.[1009] Bei Zweifeln befürworten zahlreiche Kommentierungen den Ausschluss des Legitimationstatbestands.[1010] Dies entspricht auch dem Grundsatz, dass der Verantwortliche nachweispflichtig ist, und dementsprechend den Ausnahmetatbestand nachweisen können muss.

10.1.3 Diversity-Monitoring

Das Anliegen der Diversity führt zunehmend dazu, dass auch im Unternehmenskontext ausgehend von einer KI-basierten Analyse des Ist-Zustands der Zusammensetzung der Beschäftigten, Optimierungsbedarf und Entwicklungsmöglichkeiten erarbeitet werden sollen.[1011] Da hierfür die Verarbeitung besonderer Kategorien personenbezogener Daten der Beschäftigten erforderlich sind, bestehen hohe Hürden. Andererseits nennt Art. 88 Abs. 1 DSGVO die Gleichheit und Diversität am Arbeitsplatz als einen der Gründe, für welche die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften vorsehen können.[1012] Ob der Zweck der Erstellung einer Übersicht zur Diversität im Unternehmen nach § 26 Abs. 3 Satz 1 BDSG als *erforderlich* qualifiziert werden kann, ist fraglich.[1013] Im Hinblick auf die Einholung einer ausdrücklichen Einwilligung (welche zusätzlich elektronisch/schriftlich erfolgen muss) stellt sich die Frage der Freiwilligkeit: ob bezogen auf Diversity-Kriterien ein rechtlicher Vorteil für *alle* Beschäftigten vorliegt, da bereits Art. 3 Abs. 1 GG und auch das Allgemeine Gleichbehandlungsgesetz (AGG) von einer Bestrebung nach Gleichheit ausgehen,[1014] bleibt zu diskutieren. Vorteile bestehen unfraglich bei unterrepräsentierten und schlechter bezahlten Gruppen. § 26 Abs. 2 BDSG bezieht sich auf „die beschäftigte Person“ und nicht die Beschäftigten als Gesamtheit. Insofern erscheint die Schaffung einer gesetzlichen Grundlage zur Umsetzung des Gleichbehandlungsgrundsatzes im Rahmen eines ausdifferenzierteren Beschäftigtendatenschutzes vorzugswürdiger, um Rechtssicherheit und die Umsetzung einer sehr engen Zweckbindung für derart gelagerte Fälle zu gewährleisten. Bezüglich der Option über anonymisierte Umfragen Diversity-Daten zu erheben, gilt die Menge an Daten zu berücksichtigen, d.h. die Zahl der Beschäftigten, damit Rückschlüsse auf einzelne Personen tatsächlich ausgeschlossen sind.[1015]

10.2 Datenschutz und Wettbewerb: Recht auf Datenübertragbarkeit

Einige Innovationen der DSGVO sind nicht Ausfluss der Datenschutzgrundprinzipien, stellen nichtsdestotrotz wichtige Bausteine bei der Umsetzung eines adäquaten Datenschutzkonzepts dar – je nachdem ob die Norm im konkreten Fall einschlägig ist. So haben mit dem Recht auf Datenübertragbarkeit (auch Recht auf Datenportabilität genannt) wettbewerbsrechtliche Gedanken Einzug in die DSGVO erhalten (Art. 20 DSGVO).[1016] Zielsetzung hier ist primär die Minimierung von Lock-in-Effekten, welche mittelbar Einfluss auf die effektive

[1009] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 45; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 66; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 80; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 36; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 59.

[1010] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 45; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 80; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 67; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 62.

[1011] *Krüger*, DSB 2022, 196.

[1012] *Krüger*, DSB 2022, 196 (196).

[1013] *Krüger*, DSB 2022, 196 (197). Geplante Berichtspflichten nach dem Vorschlag der EU-Kommision für eine Richtlinie hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen vom 21.04.2021, COM(2021) 189 final könnten die Erforderlichkeit der Datenerhebung künftig begründen.

[1014] So: *Krüger*, DSB 2022, 196 (197).

[1015] Vgl. Abschnitt 2.2.4.

[1016] *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 7 ff. *Jülicher u. a.*, ZD 2016, 358 (358).

Umsetzung informationeller Selbstbestimmung haben könnten.[1017] Dieses Betroffenenrecht soll den Anbieterwechsel erleichtern, indem betroffene Personen die von ihnen bereitgestellten Daten in einem strukturieren, gängigen und maschinenlesbaren Format herausverlangen können, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und mithilfe automatisierter Verfahren erfolgt. Besteht der Wunsch diese Daten an einen neuen Verantwortlichen zu übermitteln, darf der bisherige Verantwortliche dies nicht behindern. Soweit dies technisch machbar ist, darf die betroffene Person nach Art. 20 Abs. 2 DSGVO auch verlangen, dass die personenbezogenen Daten direkt vom einen zum anderen Verantwortlichen übermittelt werden. Nicht adressiert ist allerdings die Frage einer „Annahmepflicht" durch den neuen Verantwortlichen.[1018] Das langfristige Ziel dieser Regelung liegt darin, dass im Ergebnis interoperable Formate verwendet werden (vgl. ErwGr.68).[1019]

Bereitgestellte Daten: Die DSGVO enthält keine Legaldefinition für das „Bereitstellen".[1020] Nach Einschätzung des EDSA soll es sich bei den von der betroffenen Person bereitgestellten Daten einerseits um solche personenbezogene Daten handeln, die aktiv vom Benutzer eingegeben wurden.[1021] Andererseits sollen aber auch solche personenbezogene Daten als „bereitgestellt" erfasst sein, die durch Beobachtung der betroffenen Person erhoben werden können (auch als Nutzungsdaten bezeichnet).[1022] Dagegen sollen solche Daten, die der Verantwortliche aus den bereitgestellten Daten erst abgeleitet hat, nicht vom Anspruch auf Erhalt oder Übermittlung erfasst sein.[1023] Nicht betroffen sind daher solche personenbezogene Daten, die der Verantwortliche beispielsweise durch Analysen oder sonstige Verarbeitungsvorgänge gewonnen hat.[1024]

Betroffene Daten: Zudem muss betont werden, dass sich die Daten auch auf die Person beziehen müssen, die den Anspruch geltend macht und keine personenbezogenen Daten Dritter übermittelt werden. Ausgenommen vom Anwendungsbereich der Datenübertragbarkeit sind zudem anonyme bzw. anonymisierte Daten, da sie schon aus dem Anwendungsbereich der DSGVO herausfallen.[1025] Zukünftig könnte dieses Recht durch den geplanten Data-Act ausgebaut und auf nicht-personenbezogene Daten erweitert werden.[1026]

Konstellationen & Einschränkungen: Der Anspruch ist beschränkt auf Konstellationen, in denen entweder die Einwilligung oder ein Vertrag die Rechtsgrundlage zur Datenverarbeitung bilden. Datenverarbeitungen auf Grundlage anderer Erlaubnistatbestände sind explizit ausgenommen. Zudem muss die Datenverarbeitung automatisiert erfolgen. Des Weiteren dürfen bei der Weitergabe personenbezogener Daten keine Recht Dritter verletzt werden, d.h. insbesondere keine personenbezogenen Daten Dritter ohne Legitimationsgrundlage übermittelt werden.[1027] Diese Problematik bezieht sich auf die Mehrrelationalität von Daten, die über Doppel- / Drittbezug verfügen können.[1028] Würden sämtliche Daten mit Drittbezug vom Datenportabilitätsrecht ausgenommen, könnte dieses gerade in den wettbewerbspolitisch anvisierten Konstellationen

[1017] Vgl. *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 20 Rn. 2 ff. *Schantz*, NJW 2016, 1841 (1845).
[1018] *Jülicher u. a.*, ZD 2016, 358 (362); *Brüggemann*, K&R 2018, 1 (5).
[1019] So auch *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 20.
[1020] So auch *Jülicher u. a.*, ZD 2016, 358; *Brüggemann*, K&R 2018, 1 (2).
[1021] Siehe *Artikel-29-Datenschutzgruppe,* Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 9 ff.
[1022] *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 10 ff.; a.A. *Piltz,* in: Gola DS-GVO, Art. 20 Rn. 14. Siehe ausführlich zum Streit: *Westphal/Wichtermann*, ZD 2019, 191 (191 f.); *Brüggemann*, K&R 2018, 1 (2).
[1023] Hierin besteht in der Literatur Einigkeit. Siehe *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 10 ff.; *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 20 Rn. 13; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 20 Rn. 11; *Brüggemann*, K&R 2018, 1 (2); *Westphal/Wichtermann*, ZD 2019, 191 (191).
[1024] Vgl. *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 20 Rn. 11; *Brüggemann*, K&R 2018, 1 (2).
[1025] Vgl. *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 10.
[1026] Zum Entwurf siehe: *EU-Kommission,* Entwurf einer Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM 2022 68 final vom 23.2.2022.
[1027] Für eine strenge Interpretation: *Piltz,* in: Gola DS-GVO, Art. 20 Rn. 40.
[1028] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 20 Rn. 26; *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 94a.

der Social Media leer laufen.[1029] Problematisch könnte auch der Schutz von Geschäftsgeheimissen im Hinblick auf Metadaten oder Interaktionsdaten werden, wenn sich daraus Unternehmensinterna wie interne Unternehmensstrukturen oder Berechnungsmodelle der Verarbeitungsprozesse ableiten lassen.[1030] Hier wird eine umfassende Abwägung und ggf. Bereitstellung eines eingeschränkten Datensatzes empfohlen.[1031] Als technische Lösungsoptionen dieser Problematik werden der Einsatz von Algorithmen[1032] zu Trennung der Daten oder Sticky Policies[1033] zur eindeutigen Zuordnung zu einer Person vorgeschlagen. Die Artikel-29-Datenschutzgruppe schlägt hingegen Tools vor, die den betroffenen Personen ermöglichen, diejenigen Daten, die sie erhalten und übermitteln möchten, auszuwählen und etwaige Daten anderer Personen auszuschließen.[1034] Daneben könnten Verantwortliche Einwilligungsmechanismen für Drittbetroffene einführen, um im Einzelfall selbst darüber zu entscheiden, ob personenbezogene Daten mit Mehrfachbezug übertragen werden sollen.[1035]

Geltendmachung: Die betroffene Person muss bei der Geltendmachung ihres Rechts keine Formerfordernisse oder spezifische Fristen einhalten und muss keine Gründe angeben.[1036] Der Verantwortliche sollte vor der Übertragung, wie auch bei anderen Betroffenenrechten, eine sichere Identifikation der den Anspruch geltend machenden Person gewährleisten.[1037] Das Recht auf Datenübermittlung findet folglich nach Art. 11 Abs. 2 DSGVO keine Anwendung, wenn eine Identifizierung nicht möglich ist.

10.3 KI und Datentransfers in Drittländer

Nutzt ein datenschutzrechtlich verantwortliches Unternehmen ein System, welches es nicht selbst vor Ort innerhalb der EU/des EWR betreibt, sondern das von einem Dienstleister betrieben wird, der seinen Sitz außerhalb der EU/des EWR hat, muss beachtet werden, dass auch der Dienstleister die in der EU geltenden datenschutzrechtlichen Vorgaben berücksichtigt.[1038]

10.3.1 Datenübermittlung in Drittländer

Der universelle Schutzanspruch der EU-Grundrechte, insbesondere des Schutzes personenbezogener Daten nach Art. 8 EU-GrCh, wird durch die „Vererbung“ des datenschutzrechtlichen Pflichtenkanons auch beim Verlassen des territorialen Geltungsgebiets der DSGVO deutlich.[1039] Insofern werden hohe Anforderungen gesetzt, wenn personenbezogene Daten in Drittländer außerhalb der EU/des EWR übermittelt werden sollen.

10.3.1.1 Grundsätzliche Anforderungen an Drittstaatentransfers

Die Zulässigkeit des Datentransfers an Drittstaaten richtet sich nach den Art. 44 ff. DSGVO. Der Begriff des „Drittlands“ bzw. „Drittstaates“ ist in der DSGVO nicht eindeutig definiert. Im europarechtlichen Kontext wird

[1029] *Schantz*, NJW 2016, 1841 (1845).
[1030] *Jaspers*, DuD 2012, 571 (573); *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 100.
[1031] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 20 Rn. 26.
[1032] *Jülicher u. a.*, ZD 2016, 358 (362).
[1033] *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 94.1a.
[1034] *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 14.
[1035] *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 14.
[1036] Vgl. *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 62, 63; *Brüggemann*, K&R 2018, 1 (2).
[1037] *Brüggemann*, K&R 2018, 1 (2).
[1038] *BfDI*, Tätigkeitsbericht 2020, S. 32.
[1039] *Ambrock/Karg*, ZD 2017, 154 (155).

damit ein Staat bezeichnet, der nicht Mitglied der EU ist.[1040] Eine Ausnahme bilden die drei EWR-Staaten (Island, Lichtenstein, Norwegen), da diese ihre nationalen Gesetze an den EU-Rahmen angepasst haben. [1041] Übermittlung in diese Staaten sind Übermittlungen in andere EU-Mitgliedstaaten gleichgestellt.[1042] Da EU-Mitgliedstaaten als auch EWR-Staaten somit bereits an die Regelungen der DSGVO gebunden sind, finden die einen angemessenen Datenschutz oder geeignete Garantien verlangenden Art. 44 ff. DSGVO nur auf den Datentransfer in Staaten außerhalb der EU/des EWR Anwendung.[1043]

> **Art. 44 DSGVO** Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation.

Die Rechtmäßigkeit einer Datenübermittlung folgt einer Zwei-Stufen-Prüfung:[1044]

- Der Übermittlungsvorgang muss nach den allgemeinen Regeln der DSGVO rechtmäßig sein.
- Zusätzlich müssen die besonderen Bedingungen der Art. 44 ff. DSGVO erfüllt sein.

Dies bedeutet, dass zusätzlich zu den allgemeinen Regelungen zur Datenverarbeitung der DSGVO die Bestimmungen des Kapitels 5 der DSGVO (Art. 44-50 DSGVO) anzuwenden sind, um sicherzustellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen bei Datenverarbeitungen mit internationalem Kontext nicht unterschritten wird. [1045] Somit ist zu prüfen, ob ein Angemessenheitsbeschluss oder geeignete Garantien vorliegen, die die Angemessenheit des Datenschutzniveaus gewährleisten.[1046] Sollte dabei festgestellt werden, dass keine von beiden Voraussetzungen gegeben sind, kann eine Prüfung der Ausnahmevorschriften erfolgen.[1047]

10.3.1.1.1 Datenübermittlung in Drittstaaten mit einem angemessenen Schutzniveau

Liegt ein Angemessenheitsbeschluss der EU-Kommission vor, handelt es sich um einen Drittstaat mit angemessenem Schutzniveau und eine Datenübermittlung darf ohne weitere Genehmigung erfolgen (Art. 45 Abs. 1 S. 2, ErwGr. 103 S. 2).[1048]

> **Art. 45 Abs. 1 DSGVO** Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes

[1040] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 44 Rn. 6; *Kamp/Beck,* in: BeckOK DatenschutzR Art. 44 Rn. 23.
[1041] *Kamp/Beck,* in: BeckOK DatenschutzR Art. 44 Rn. 24.
[1042] *Kamp/Beck,* in: BeckOK DatenschutzR Art. 44 Rn. 24.
[1043] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 44 Rn. 17; *Auer-Reinsdorff/Conrad*, Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Grenzüberschreitende Datenverarbeitung, Rn. 20.
[1044] *Ambrock/Karg*, ZD 2017, 154 (155); *Voigt/von dem Bussche,* in: Konzerndatenschutz, Kap. 3 Rn. 1.
[1045] *Ambrock/Karg*, ZD 2017, 154 (155).
[1046] *Ambrock/Karg*, ZD 2017, 154 (156).
[1047] *Ambrock/Karg*, ZD 2017, 154 (156).
[1048] *Beck,* in: BeckOK DatenschutzR Art. 45 Rn. 1; *Ambrock/Karg*, ZD 2017, 154 (156).

Schutzniveau bietet. Eine solche Datenübermittlungen bedarf keiner besonderen Genehmigung.

Die EU-Kommission hat eine Reihe von Staaten mit einem angemessenen Schutzniveau anerkannt. Im Einzelnen handelt es sich derzeit um die folgenden Staaten: [1049] Andorra (Kommissionsbeschluss 2010/625/EU vom 19.10.2010, ABl. EU vom 21.10.2010, Nr. L 277/27), Argentinien (Kommissionsbeschluss 2003/490/EG vom 30.03.2003, ABl. EG vom 5.7.2003, Nr. L 168/19), Australien, Sonderfall PNR-Daten (ABl. EU v. 8.8.2008, Nr. L 213/47), Canada (Kommissionsbeschluss 2002/2/EG vom 20.12.2001, ABl. EG vom 4.1.2002, Nr. L 2/13.), Färöer-Inseln (Kommissionsbeschluss 2010/146/EG vom 05.03.2010, ABl. EU vom 9.3.2010, Nr. L 58/17.), Großbritannien (Kommissionsbeschluss C(2021) 4800 final vom 28.06.2021), Guernsey (Kommissionsbeschluss 2003/821/EC vom 21.11.2003, ABl. EG vom 25.11.2003, Nr. L 308/27.), Isle of Man (Kommissionsbeschluss 2004/411/EC vom 28.04.2004, ABl. EU vom 30.4.2004, Nr. L 151/51), Israel (Kommissionsbeschluss 2011/61/EU vom 31.01.2011, ABl. EU vom 1.2.2011, Nr. L 27/39.), Japan (Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23.1.2019, ABl. vom 19.3.2019, Nr. L 76/1) [1050], Jersey (Kommissionsbeschluss 2008/393/EC vom 08.05.2008, ABl. EU vom 28.5.2008, Nr. L 138/21.), Neuseeland (Kommissionsbeschluss 2013/65/EU vom 19.12.2012, ABl. EU vom 30.1.2013, Nr. L 28/12.), Schweiz (Kommissionsbeschluss 2000/518/EC vom 26.07.2000, ABl. EG vom 25.8.2000, Nr. L 215/1.), Südkorea (Kommissionsbeschluss C(2021) 9316 final vom 17.12.2021), Uruguay (Kommissionsbeschluss 2012/484/EU vom 21.08.2012, ABl. EU vom 23.8.2012, Nr. L 227/11.)

Bei diesen Staaten ist es nicht mehr erforderlich, in eine Prüfung einzutreten, ob diese ein angemessenes Datenschutzniveau aufweisen. Als Folge ist eine Datenübermittlung in diese Staaten ohne eine weitere eigene Überprüfung datenschutzrechtlich zulässig. Allerdings ist aus den obengenannten Angemessenheitsbeschlüssen zu erkennen, dass diese Entscheidungen der EU-Kommission relativ lange zurückliegen (zwischen 2000-2013, als die DSGVO noch nicht existierte). Die EU-Kommission ist nach dem Inkrafttreten der DSGVO verpflichtet, alle Angemessenheitsbeschlüssen dahingehend zu überprüfen, ob in den jeweiligen Staaten ein der EU vergleichbares Datenschutzniveau anerkannt werden kann. [1051]

10.3.1.1.2 Datenübermittlung vorbehaltlich angemessener Garantien

Liegt kein Angemessenheitsbeschluss vor, können Garantien die Angemessenheit des Datenschutzniveaus gewährleisten (Art. 46, 47 DSGVO). Fehlen auch diese, kommen einige Ausnahmen in Betracht (Art. 49 DSGVO). Dabei sind die Vorschriften mit dem Ziel anzuwenden und auszulegen, dass das durch die DSGVO gewährleistete Schutzniveau auch bei Datenübermittlungen im internationalen Kontext aufrechterhalten wird. [1052] Der Ausdruck „angemessenes Schutzniveau“ bedeutet nach der Rechtsprechung des EuGHs dabei nicht, dass das Drittland ein identisches Schutzniveau gewährleisten muss, es wird aber verlangt, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union im Licht des in der Grundrechtecharta garantierten Niveaus der Sache nach gleichwertig ist. [1053]

Garantien: Wenn kein Angemessenheitsbeschluss durch die EU-Kommission vorliegt, ist gemäß Art. 46 Abs. 1 DSGVO zu prüfen, ob andere geeignete Garantien für eine Datenübermittlung in die betreffenden Dritt-

[1049] Beschlüsse abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [letzter Abruf 18.08.2021].
[1050] Erster Angemessenheitsbeschluss nach Inkrafttreten der DSGVO.
[1051] EU Commission, Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [letzter Abruf 28.05.2021].
[1052] *Ambrock/Karg*, ZD 2017, 154 (156).
[1053] EuGH, Urteil vom 06.10.2015 – C-362/14 – Schrems I, Rn. 73.

staaten vorliegen. Als zusätzliche Bedingung müssen die betroffenen Personen auf Grundlage dieser Garantien durchsetzbare Rechte zugestanden werden und wirksame Rechtsbehelfe zur Verteidigung dieser Rechte bestehen.[1054] In Art. 46 Abs. 2 DSGVO ist eine nicht abschließende Aufzählung geeigneter Garantien aufgelistet, bei deren Vorliegen Daten übermittelt werden dürfen, ohne dass hierzu noch eine besondere Genehmigung einer Aufsichtsbehörde notwendig ist. Das sind folgende Instrumente:

- Rechtlich bindende und durchsetzbare Verwaltungsvereinbarungen
- Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) gemäß Art. 47 DSGVO
- Standarddatenschutzklauseln der EU-Kommission (Standardvertragsklauseln)
- Genehmigte Verhaltensregeln nach Art. 40 DSGVO und genehmigte Zertifizierungsmechanismen nach Art. 42 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen

Vorbehaltlich der Genehmigung der zuständigen Aufsichtsbehörde können Garantien zudem bestehen in:

- Einzeln ausgehandelte Vertragsklauseln und
- Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen

Aus Unternehmensperspektive sind die Standardvertragsklauseln (engl. Standard Contractual Rules, SCC) und genehmigten verbindlichen internen Datenschutzvorschriften (engl. Binding Corporate Rules, BCR) die relevantesten Fallgruppen:

Standard Contractual Clauses (SCC) Hierbei handelt es sich um von der EU-Kommission „vorgenehmigte“ Mustervertragsklauseln über die sichergestellt werden soll, dass Vertragspartner im Drittstaat ein angemessenes Schutzniveau einhalten.[1055] Im Juni 2021 veröffentlichte die Kommission modernisierte Standardvertragsklauseln unter der DSGVO für Datenübertragungen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, die der DSGVO unterliegen, an nicht der DSGVO-unterliegende Verantwortliche oder Auftragsverarbeiter (insbesondere mit Sitz außerhalb der EU/des EWR).[1056] Bei individuell ausgehandelten Vertragsklauseln nach Art. 46 Abs. 3 Buchst. a DSGVO bedarf es einer Genehmigung durch die zuständige Aufsichtsbehörde. Bei der Nutzung der SCC ist hingegen keine weitere Genehmigung erforderlich.[1057] Im Rahmen der SCC ist ausdrücklich festzulegen, welche Vertragsparteien in welchen Rollen beteiligt sind (Datenexporteur und Datenimporteur), sowie nach Möglichkeit die konkreten Datenflüsse den jeweiligen Vertragsparteien eindeutig zuzuordnen.[1058] SCC gehen von einem Vertragsmodell aus, in welchem die Vertragspartner die Einhaltung der Vertragsklauseln überwachen.[1059] Der EuGH hatte die bisher geltenden, bereits unter der Datenschutz-Richtlinie erlassenen SCC als gültig bestätigt, dabei aber anklingen lassen, dass diese nicht für jeden denkbaren Fall des Datentransfers in Drittländer schon alle zur Herstellung eines gleichwertigen Datenschutzniveaus erforderlichen Vereinbarungen und Maßnahmen enthalten (insbesondere können sie aufgrund ihres Vertragscharakters keine drittstaatlichen Behörden binden), sondern in Abhängigkeit von der Rechtslage im Empfängerland insbesondere hinsichtlich von Datenzugriffen dortiger Behörden gegebenenfalls durch zusätzliche Maßnahmen ergänzt werden müssen.[1060]

[1054] *Ambrock/Karg*, ZD 2017, 154 (156). So auch die Feststellungen des EuGHs zum Safe-Harbour-Abkommen: EuGH, Urteil vom 06.10.2015 – C-362/14 – Schrems I, Rn. 95.
[1055] *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 13.
[1056] Abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de [letzter Abruf 18.08.2021].
[1057] *Voigt/von dem Bussche,* in: Konzerndatenschutz, Kap. 3 Rn. 1; *Schantz,* in: NK Datenschutzrecht Art. 46 Rn. 31.
[1058] *Voigt/von dem Bussche,* in: Konzerndatenschutz, Kap. 3 Rn. 5.
[1059] *Schantz,* in: NK Datenschutzrecht Art. 46 Rn. 35.
[1060] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 132 ff.; *Lange/Filip,* In: BeckOK DatenschutzR Art. 46 Rn. 25; *Schwartmann/Burkhardt*, ZD 2021, 235 (235); *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12a ff.

Binding Corporate Rules (BCR): bieten Spielräume für multinationale Konzerne für grenzüberschreitende Datentransfers innerhalb von Konzernunternehmen.[1061] Eine genaue Definition bietet Art. 4 Nr. 20 DSGVO. Solche Regeln müssen alle allgemeinen Datenschutzgrundsätze und einklagbare Rechte enthalten, um angemessene Garantien für Datenübertragungen zu gewährleisten.[1062] Sie müssen rechtsverbindlich sein und von jedem betroffenen Mitglied der Unternehmensgruppe durchgesetzt werden.[1063] Die Unternehmen müssen der zuständigen Datenschutzbehörde BCR zur Genehmigung vorlegen, welche dann nach dem Kohärenzverfahren gemäß Art. 63 DSGVO erfolgt. BCR kommen folglich nur in Frage, wenn die Kommunikation unternehmensintern erfolgt.

10.3.1.1.3 Ausnahmen für bestimmte Fälle

Falls weder ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt noch geeignete Garantien nach Art. 46 DSGVO bestehen, ist eine Übermittlung personenbezogener Daten in ein Drittland nur auf Basis der in Art. 49 Abs. 1 DSGVO genannten Ausnahmen zulässig. Der Ausnahmekatalog aus dem Art. 49 Abs. 1 S. 1 Buchst. a-g DSGVO lautet wie folgt:

- Ausdrückliche Einwilligung der betroffenen Person nach Unterrichtung
- Erforderlichkeit zur Erfüllung eines Vertrags mit der betroffenen Person oder zur Durchführung vorvertraglichen Maßnahmen
- Erforderlichkeit zum Abschluss oder zur Erfüllung eines Vertrags im Interesse der betroffenen Person mit einer anderen Person
- Zur Wahrung eines wichtigen öffentlichen Interesses
- Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Zum Schutz lebenswichtiger Interessen bei Unmöglichkeit einer Einwilligung
- Daten aus Registern zur Information der Öffentlichkeit
- Begrenzte Übermittlung nach Interessenabwägung bei „zwingenden berechtigten Interessen“ (Art. 49 Abs. 1 S. 2 DSGVO)

Einwilligung: Die Wirksamkeit und damit die einen Datentransfer in ein unsicheres Drittland legitimierende Wirkung der Einwilligung setzt voraus, dass die betroffene Person

(1) über bestehende Risiken derartiger Datenübermittlungen
(2) ohne Vorliegen eines Angemessenheitsbeschlusses und geeigneter Garantien unterrichtet wurde und
(3) in Kenntnis dieser Umstände *ausdrücklich* einwilligt.[1064]

Umstritten ist hierbei, wie weit über die Rechtslage im Zielland informiert werden muss.[1065] So verlangen einige Literaturstimmen, konkrete Erkenntnisse zu Datenmissbrauchsrisiken oder typische Risiken wie z.B. erschwerte Durchsetzung von Betroffenenrechten, fehlende Kontrolle der Weiterverarbeitung und Übermitt-

[1061] *Voigt,* in: Konzerndatenschutz, Kap. Rn. 15.
[1062] *Schneider,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 2 Rn. 158.
[1063] *Towfigh/Ulrich,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 47 Rn. 14 ff.
[1064] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 4 f.
[1065] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 8.

lung der Daten, fehlende Datenschutzaufsicht oder Zugriffe durch staatliche Stellen den betroffenen Personen vor Augen zu führen.[1066] Anderen genügt abstrakt auf das Risiko eines fehlenden angemessenen Datenschutzniveaus und fehlender Garantien zu verweisen.[1067] Der EDSA verlangt als Beispiele die konkrete Information über ein mögliches Fehlen von Aufsichtsbehörden, von Datenverarbeitungsgrundsätzen oder von Datenschutzrechten der betroffenen Personen.[1068]

Umstritten ist ferner, ob die Einwilligungsfähigkeit ausscheiden muss, wenn der Wesensgehalt der Grundrechte der Art. 7, 8 EU-GrCh betroffen ist, also eine Missachtung fundamentaler und grundlegender Rechte der Betroffenen zu befürchten ist.[1069] Da die Einwilligung das Instrument zur Wahrnehmung der eigenen Autonomie und eigener Gestaltungsinteressen bietet, ist bei Überlegungen zur Einschränkbarkeit der Einwilligung Vorsicht geboten.[1070] Andererseits wird gerade bei „leicht" erteilten Einwilligungen die bloße Fiktion der Freiwilligkeit bemängelt.[1071] Insofern ist es bedeutsam, dass die Auslegung und Anwendung der Regelungen zur Einwilligung stets im Lichte der Autonomiesicherung dem Selbstbestimmungsgedanken Rechnung trägt.[1072] Wesentliche Kriterien hierfür sind die Informiertheit, Freiwilligkeit und Reversibilität.[1073] Ist eine Entscheidung (rechtlich oder zumindest praktisch) unabänderlich, wäre es durchaus diskutierbar, neben einer ausdrücklichen Einwilligung weitere Schutzmaßnahmen zu fordern.[1074] Andererseits wäre ebenfalls eine Autonomieeinschränkung gegeben, wenn betroffenen Personen das Recht abgesprochen würde, die sie betreffenden Daten zu teilen.[1075] Diesen Gedanken reflektiert Art. 9 Abs. 2 Buchst. e DSGVO bei der Veröffentlichung besonderer Kategorien personenbezogener Daten. Folglich kann betroffenen Personen nicht verwehrt werden, auch aus einem unsicheren Drittland betriebenen Dienste ohne besondere Schutzgarantien zu nutzen, solange sie tatsächlich ausreichend über diesen Umstand informiert sind. Dementsprechend erscheint es auch sachgerecht einen strengen Maßstab an die Bereitstellung der Information zu stellen.

Im Hinblick auf Beschäftigten stellt sich wiederum die Frage der Freiwilligkeit, also ob sie eine echte Wahl haben und ohne Nachteile zu erleiden die Einwilligung verweigern oder widerrufen können. [1076] Die Übertragung des Grundsatzes der differenzierten Einwilligung auf die Auswahl von Zielländern dürfte zwar zu weit

[1066] *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 14; *Ambrock/Karg*, ZD 2017, 154 (157).
[1067] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 49 Rn. 6; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 15.
[1068] *European Data Protection Board*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 9.
[1069] *Ambrock/Karg*, ZD 2017, 154 (158).
[1070] Vgl. zu Verboten zum Schutz der Menschenwürde: VG Neustadt, NVwZ 1993, 98 – Zwergenweitwurf, BVerwGE 64, 274 – Peepshow I; BVerwGE 115, 189 – Omega, welche selbst wiederum dem Vorwurf eines Eingriffs in die Menschenwürde ausgesetzt sind: VG Weimar, Urteil vom 06.04.2016 – 3 K 1422/14 We, Rn. 18; vgl. auch OVG Lüneburg, Urteil vom 18.02.2010 – 1 LC 244/07, Rn. 71.
[1071] *Buchner/Kühling*, DuD 2017, 544 (545); *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 108; *Kamp/Rost*, DuD 2013, 80 (82); *Krauß u. a.*, DuD 2017, 217 (219); *Rihaczek*, DuD 2003, 667 (667); *Roßnagel u. a.*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, S. 91; *Seidel*, ZG 2014, 153 (155); *Simitis*, NJW 1984, 398 (401); *Veil*, NVwZ 2018, 686 (688).
[1072] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 174 ff.; 307 ff.
[1073] *Picot u. a.*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 169 (174).
[1074] Neben der Sicherung von Individualrechten kommt dem Datenschutz auch ein objektiv-rechtlicher Gehalt zu: *Bäcker*, Der Staat 2012, 91 (95); *Boehme-Neßler*, International Data Privacy Law 2016, 222 (226); *Winter*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 37 (46).
[1075] Gewisse Beschränkungen wären hingegen mit dem Argument der Mehrrelationalität möglich: Daten beziehen sich oftmals nicht nur auf eine betroffene Person, sondern erlauben oftmals Rückschlüsse auf weitere Betroffene, vgl. *Wagner*, Datenökonomie und Selbstdatenschutz, S. 200 f.
[1076] *Schwartmann/Burkhardt*, ZD 2021, 235 (236); *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 11; *Schantz,* in: BeckOK DatenschutzR Art. 49 Rn. 16; *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 49 Rn. 10; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 16; *Ambrock/Karg*, ZD 2017, 154 (157). Von einer echten Wahl bei karriereförderndenVerarbeitungsvorgängen ausgehend: *Klug,* in: Gola DS-GVO, Art. 49 Rn. 5.

gehen, da dann eine Datenverarbeitung jeweils in und außerhalb der EU angeboten werden müsste.[1077] Allerdings eignet sich die Einwilligung wegen ihrer Widerruflichkeit nicht für wiederholte, routinemäßige oder systematische Datenübermittlungen.[1078]

Sonstige Ausnahmen im Beschäftigtenkontext: Im Hinblick auf die Erforderlichkeit zur Erfüllung des Arbeitsvertrags gelten ebenfalls strenge Maßstäbe: Nützlichkeit alleine reicht nicht aus, es müsste ein „direkter und objektiver Zusammenhang“ zum Vertrag bestehen und zudem ist fraglich, ob „Ausnahmen für bestimmte Fälle“ über Einzelausnahmen hinausgehen und damit wiederkehrende Übermittlungen legitimieren können.[1079] Stimmen aus der Literatur sehen hingegen dort den Ausnahmecharakter als erfüllt an, wenn die Pflege zu Auslandskontakten in Drittländern und damit die Übermittlung von Daten bereits im Arbeitsvertrag zwischen Beschäftigten und Unternehmen hinreichend deutlich zum Ausdruck kommt, bspw. wenn Beschäftigte spezifisch für Einkaufs- oder Verkaufskontakte mit Drittländern eingestellt wurden.[1080] Umstritten ist, ob bei Matrixstrukturen, auch regelmäßige Kommunikation zwischen konzernangehörigen Einheiten wie bspw. Berichtspflichten an Fachvorgesetze in internationalen Konzernstrukturen auf Grundlage des Arbeitsvertrags erfüllt sowie konzernweite Kontaktdatenverzeichnisse gepflegt werden dürfen.[1081] Kritisiert wird hierbei, dass keine „gelegentliche“ Übermittlung mehr gegeben wäre (vgl. ErwGr. 111 S. 1 DSGVO).[1082] Im Ergebnis ist davon auszugehen, dass wiederholte, gleichgelagerte Übermittlungen innerhalb von Konzernen und Unternehmensgruppen auf geeignete Garantien nach Art. 46 DSGVO gestützt werden sollten oder unterbleiben müssten.[1083]

Ein regelmäßiger Einsatz eines KI-Systems, das einen Drittstaatentransfer erfordert, wäre auch nicht über „zwingende berechtigte Interessen“ legitimierbar, da wiederholte oder routinemäßige Übermittlungen explizit nicht darunter fallen sollen.[1084] Mindestens wären geeignete und angemessene Schutzgarantien zu ergreifen. Da es sich bei der Interessenabwägung in diesem Kontext um eine „Ausnahme unter den Ausnahmen“ handelt,[1085] dürfte sie in der Praxis kaum Drittlandübermittlungen rechtfertigen.[1086]

[1077] *Schantz,* in: BeckOK DatenschutzR Art. 49 Rn. 18. *Ambrock/Karg* sprechen demgegenüber von zwei getrennten Einwilligungen: in den Datenverarbeitungsvorgang selbst und in den Drittstaatentransfer: *Ambrock/Karg*, ZD 2017, 154 (158). Sind beide Vorgänge untrennbar verknüpft, dürfte der ersten Einwilligung allerdings keinerlei Bedeutung zukommen.

[1078] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 11. Aufgrund des Ausnahmecharakters gehen *Ambrock/Karg* darüber hinaus davon aus, dass Art. 49 DSGVO nur für Ausnahmesituationen mit einmaligem Charakter einschlägig sei: *Ambrock/Karg*, ZD 2017, 154 (157). Dies würde durch die im Singular formulierten Erwägungsgründe 111-113 deutlich.

[1079] *European Data Protection Board*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 10; *Schwartmann/Burkhardt*, ZD 2021, 235 (236); *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 19; *Rohrlich*, ZAP 2020, 1265 (1269).

[1080] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 15; *Gabel,* in: Taeger/Gabel - DSGVO/BDSG Art. 49 Rn. 8.

[1081] bejahend: *Klug,* in: Gola DS-GVO, Art. 49 Rn. 6; *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 23; *Gabel,* in: Taeger/Gabel - DSGVO/BDSG Art. 49 Rn. 8.

[1082] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 16.

[1083] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 16; ähnlich *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 24; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 19.

[1084] *Klug,* in: Gola DS-GVO, Art. 49 Rn. 12; *Pauly* in: Paal/Pauly - DS-GVO BDSG Art. 49 Rn. 28; *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 32.

[1085] *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 52.

[1086] *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 34.

Der Europäische Datenschutzausschuss veröffentlichte Hilfestellungen im Hinblick auf Drittstaatentransfers:[1087]

European Data Protection Board, Recommendations 01/2020

- **Schritt 1:** Kenne deine Datentransfers
- **Schritt 2:** Identifiziere die Transferregeln (Angemessenheitsbeschluss, SCC, BCR, etc.)
  - ➔ Sichern diese ein im Wesentlichen gleichwertiges Schutzniveau?
- **Schritt 3:** Bewerte, ob das Übermittlungsinstrument nach Art. 46 DSGVO, auf das sich der Transfer stützt, unter Berücksichtigung aller Umstände des Einzelfalls wirksam ist.
  - ➔ Unterliegt der Empfänger im Drittland Rechtsvorschriften und Praktiken, welche die Durchsetzung der Datenschutzrechte hindern?
- **Schritt 4:** Umsetzung von Zusatzschutzmaßnahmen: diese sollten technischer Natur sein und können durch vertragliche und/ oder organisatorische Maßnahmen ergänzt werden
  - ➔ Die Auswahl orientiert sich an den zu kompensierenden Risiken um Drittland sowie Art und Umfang der Datenübermittlung
- **Schritt 5:** Umsetzung der Verfahrensschritte, inkl. wirksamer zusätzlicher Maßnahmen (ggf. Einholung erforderlicher Erklärungen/Genehmigungen, etc.)
- **Schritt 6:** Re-Evaluation in angemessenen Abständen

Als nicht abschließende Beispiele technischer Maßnahmen – welche je nach Kontext und spezifischer Schutzwirkung auszuwählen sind – nennt der EDSA folgende Maßnahmen:[1088]

- **Verschlüsselung:** Bei Datenspeicherung für Sicherungszwecke und andere Zwecke, die keinen Zugriff auf die Daten im Klartext erfordern: Nutzung eines Verschlüsselungsalgorithmus, der z. B. im Hinblick auf Schlüssellänge, Betriebsmodus, etc. dem Stand der Technik entspricht und robust gegen Brute-Force-Angriffe ist. Die Stärke der Verschlüsselung und die Schlüssellänge müssen dem spezifischen Zeitraum Rechnung tragen, in dem die Vertraulichkeit der verschlüsselten personenbezogenen Daten gewahrt bleiben muss. Der Verschlüsselungsalgorithmus muss korrekt und durch ordnungsgemäß gewartete Software ohne bekannte Schwachstellen implementiert sein, deren Konformität mit der Spezifikation des gewählten Algorithmus überprüft wurde, z. B. durch Zertifizierung. Die Schlüssel müssen zuverlässig verwaltet werden und dürfen ausschließlich in der Kontrolle des Datenexporteurs stehen.

[1087] *European Data Protection Board*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.
[1088] *European Data Protection Board*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, S. 28 ff.

- **Pseudonymisierung:** in einer Weise, dass die personenbezogenen Daten weder einer bestimmten betroffenen Person zugeordnet werden können noch dazu verwendet werden können, die betroffene Person ohne die Verwendung zusätzlicher Informationen aus einer größeren Gruppe herauszugreifen. Identifizierende Informationen dürfen ausschließlich beim Exporteur vorhanden sein und durch diesen kontrolliert werden. Die Weitergabe oder unbefugte Nutzung dieser zusätzlichen Informationen muss durch geeignete technische und organisatorische Garantien verhindert werden. Der Verantwortliche muss durch eine gründliche Analyse der betreffenden Daten feststellen, dass die pseudonymisierten Daten auch bei einem Abgleich mit sonstigen Informationen nicht einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

European Data Protection Board, Recommendations 01/2020

- Es ist zu beachten, dass in vielen Situationen Faktoren, die für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität einer natürlichen Person, ihren physischen Standort oder ihre Interaktion mit einem internetbasierten Dienst zu bestimmten Zeitpunkten spezifisch sind, die Identifizierung dieser Person ermöglichen können, auch wenn ihr Name, ihre Adresse oder andere eindeutige Identifikatoren weggelassen werden. Dies gilt insbesondere dann, wenn die Daten die Nutzung von Informationsdiensten betreffen (Zeitpunkt des Zugriffs, Reihenfolge der abgerufenen Funktionen, Merkmale des verwendeten Geräts usw.). Diese Dienste könnten, wie der Importeur personenbezogener Daten, verpflichtet sein, denselben Behörden in ihrem Zuständigkeitsbereich Zugang zu gewähren, die dann wahrscheinlich über Daten über die Nutzung dieser Informationsdienste durch die Zielperson(en) verfügen werden.

- **Transportverschlüsselung:** sofern Gefahren eines unzulässigen Datenzugriffs den Transportweg betreffen und die Verschlüsselungsprotokolle dem Stand der Technik entsprechen sowie wirksamen Schutz gegen aktive und passive Angriffe mit bekannten Mitteln bieten und entsprechende Sicherheitsgarantien eingehalten werden können (bspw. vertrauenswürdige Zertifizierung, Infrastruktur, Angriffsschutz, Schwachstellentests, etc.).
- **Split oder Multi-Party Processing:** Die Daten werden zwischen unabhängigen Auftragsverarbeitern in unterschiedlichen Rechtsordnungen so aufgeteilt, dass kein Teil, den ein einzelner Verarbeiter erhält, ausreicht, um die personenbezogenen Daten ganz oder teilweise zu rekonstruieren und damit Personen zu identifizieren. Der Datenexporteur erhält das Ergebnis der Verarbeitung von jedem der Auftragsverarbeiter unabhängig und fügt die erhaltenen Teile zusammen, um das Endergebnis zu erhalten, das personenbezogene oder aggregierte Daten darstellen kann. Hierfür können auch sicherer Mehrparteienberechnungen zum Einsatz kommen, und zwar so, dass keinem von ihnen Informationen offenbart werden, die sie nicht schon vor der Berechnung besitzen. Der für die gemeinsame Berechnung verwendete Algorithmus muss gegen aktive Angreifer sicher sein. Der Verantwortliche muss nachweisen können, dass selbst mit Abgleich weiterer (im Drittland) verfügbarer Daten, kein Personenbezug hergestellt werden kann.

10.3.2 Datenzugriffe aus Drittländern: Beispiel USA

10.3.2.1 Datenübermittlung in die USA

Im Hinblick auf Datenübermittlungen in die USA besteht die Problematik, dass kein einheitlich normiertes Datenschutzrecht existiert und auch kein den EU-Standards entsprechendes angemessenes Datenschutzniveau angenommen werden kann.[1089] Versuche dies über Abkommen („Safe Harbour“, „Privacy Shield“) zu lösen, scheiterten wiederholt.[1090] Der EuGH begründet seine Entscheidungen damit, dass das US-Recht – insbesondere die Überwachungsprogramme und Zugriffsbefugnisse der US-Behörden, welche nach Ansicht des EuGHs unverhältnismäßig geregelt sind, – für die vom US-Recht adressierten Datenverarbeiter gegenüber den Grundsätzen des Privacy Shield Vorrang genießen.[1091] Daraus folgt, dass es an wirksamen Rechtsschutzinstrumenten für EU-Bürger*innen mangele, gegen Maßnahmen von US-Behörden vorzugehen und Rechte durchzusetzen.[1092] Die Entscheidung führt zur Rechtsfolge, dass Datenübermittlungen, die bis dahin auf Grundlage des Privacy Shield-Abkommens erfolgten, nun entweder auf eine andere alternative Rechtsgrundlage gestützt oder ausgesetzt werden müssen.[1093]

Im Hinblick auf den Einsatz von Standardvertragsklauseln betonte der EuGH, dass es dem Verantwortlichen bzw. seinem Auftragsverarbeiter obliegt, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren.[1094] Sie sind verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden, wenn das Recht dieses Drittlands dem Empfänger aus der Union übermittelter personenbezogener Daten Verpflichtungen auferlegt, die den genannten Klauseln widersprechen und daher geeignet sind, die vertragliche Garantie eines angemessenen Schutzniveaus hinsichtlich des Zugangs der Behörden dieses Drittlands zu diesen Daten zu untergraben.[1095] Damit etablierte der EuGH eine fortlaufende Prüfpflicht des Verantwortlichen in Zusammenarbeit mit dem Empfänger, das Recht sowie Entwicklungen des Rechts im Bestimmungsland zu analysieren und dabei besonderes Augenmerk auf die nationalen Sicherheitsgesetze des jeweiligen Bestimmungsdrittlands und deren praktische Handhabung zu legen.[1096] Im Anschluss an die Entscheidung betonte der EDSA die einzelfallbezogene Überprüfung des Datenschutzniveaus in dem betreffenden Drittland auf seine Angemessenheit, wofür die Kriterien des Art. 45 Abs. 2 DSGVO als Maßstab herangezogen werden können, sowie die Berücksichtigung der Umstände der Übermittlung sowie potentiell einzubeziehende Maßnahmen.[1097] Die DSK kommt zur Ansicht, dass Standarddatenschutzklauseln ohne zusätzliche Maßnahmen für Datenübermittlungen in die USA

[1089] *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 8; ausführlich zum Privacy Shield: *Spies,* in: Konzerndatenschutz, Kap. 3.
[1090] EuGH, Urteil vom 06.10.2015 – C-362/14 – Schrems I; EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II.
[1091] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 163 ff.
[1092] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 176 ff.
[1093] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 45 Rn. 24c.
[1094] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 134.
[1095] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 135
[1096] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12b.
[1097] *European Data Protection Board*, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, S. 2 ff.; *Schwartmann/Burkhardt*, ZD 2021, 235 (235).

grundsätzlich nicht mehr ausreichend seien.[1098] Insbesondere wird angesichts der Rechtslage in den USA bezweifelt, dass Regelungen der SCC vor Ort wirksam durchsetzbar sind.[1099] Eine Schritt-für-Schritt-Anleitung zur Umsetzung der Prüfungspunkte inklusiver grafischer Übersicht wird vom Landesdatenschutzbeauftragten für Rheinland-Pfalz bereitgestellt.[1100] Schlussendlich wird konstatiert, der EuGH habe Datenübermittlungen in die USA unter SCC unter kaum erfüllbare Bedingungen gestellt.[1101] Diese Wertungen der Schrems-II-Entscheidung sind auch auf andere Garantien nach Art. 46 DSGVO genannten Garantien übertragbar, sodass diese auch bei Binding Corporate Rules Anwendung finden dürften.[1102]

Unklar war, welche zusätzlichen Maßnahmen eine Datenübermittlung in die USA legitimieren können. Der EuGH hat diese Frage offengelassen.[1103] Vertragliche Lösungen allein dürften auch nach Ansicht des EDSA ausscheiden.[1104] Technische Maßnahmen wie Verschlüsselung und/oder Pseudonymisierung könnten Risiken gegenüber Zugriffen drittstaatlicher Behörden mitigieren.[1105]

Zusammenfassend bliebt festzuhalten:

- Für Datenübermittlungen in die USA besteht kein Angemessenheitsbeschluss oder Äquivalent.
- Der Abschluss von Standardvertragsklauseln und Binding Corporate Rules reichen allein nicht aus, um Datenübermittlungen in die USA zu legitimieren. Zusätzlich muss über geeignete technische und/oder organisatorische Maßnahmen auch sichergestellt werden, dass diese eingehalten werden können.

10.3.2.2 Datenzugriffe aus den USA

Ebenso problematisch wie nach EU-Recht als unzulässig zu bewertende Zugriffe auf Daten *in* Drittländern (insbesondere durch lokale Behörden), sind solche Zugriffe *aus* Drittländern auf personenbezogene Daten, die innerhalb der EU bzw. des EWR verarbeitet werden.

Ob eine Lösung der Datenübermittlungsproblematik für US-amerikanische Kommunikations- und Cloudanbieter über eine Verortung der gesamten Serverinfrastruktur innerhalb der EU (des EWR) gesucht werden kann, erscheint ebenfalls fraglich. Denn im Wege des sog. CLOUD-Acts („Clarifying Lawful Overseas Use of Data Act“) könnte von US-amerikanischen Unternehmen durch Ermittlungsbehörden verlangt werden, dass (auch personenbezogene) Kundendaten an amerikanische Behörden preisgegeben werden müssen, unabhängig davon, wo die Daten gehostet werden.[1106] Das Sicherheitsproblem, welches zur Feststellung des nicht

[1098] DSK, Pressemitteilung vom 28.7.2020: Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“) stärkt den Datenschutz für EU-Bürgerinnen und Bürger; abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf [letzter Abruf 18.08.2021].
[1099] *Rohrlich*, ZAP 2020, 1265 (1269).
[1100] Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Datenübermittlung in Drittländer, Stand: 24.7.2020; abrufbar unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/datenuebermittlung-in-drittlaender/, sowie grafische Übersicht unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf [letzter Abruf 18.08.2021].
[1101] *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1102] *Pauly*, in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12d.
[1103] *Pauly*, in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12a; *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1104] *European Data Protection Board*, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, S. 5; *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1105] *European Data Protection Board*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.
[1106] *Schwartmann/Burkhardt*, ZD 2021, 235 (236); *Gausling*, MMR 2018, 578 (579).

angemessenen Schutzniveaus in den USA führte,[1107] bleibt folglich bestehen. Unternehmen könnten in den USA zu einer Datenübermittlung verpflichtet werden, die nicht mit EU-Recht vereinbar ist.[1108] Adressaten des CLOUD-Acts sind Anbieter elektronischer Kommunikationsdienste sowie Remote-Computing-Dienste, die US-Recht unterfallen.[1109] Gleichzeitig fordert Art. 48 DSGVO, das Datenübermittlungsersuchen drittstaatlicher Behörden auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sein müssen, um anerkannt und vollstreckt zu werden. Ein solches Rechtshilfeabkommen sieht der CLOUD-Act hingegen nicht als Bedingung.[1110] Die Heranziehung anderer Legitimationsgrundlagen kommt nach Einschätzung des Europäischen Datenschutzausschusses und dem Europäischen Datenschutzbeauftragten (mit Ausnahme extrem gelagerter Einzelfälle) in der Regel kaum zur Zulässigkeit einer Datenübermittlung.[1111] Daher wird auch hier geschlussfolgert, dass für die Legitimation von Kommunikations- oder Cloud-Angeboten die Lösung ausschließlich über eine europäische Datenverarbeitung durch Serverstandorte in der EU nicht funktioniert. [1112] Zusätzlich müssten weitere technischen oder organisatorischen Maßnahmen ergriffen werden. Als Lösungsoptionen werden im Schrifttum unterschiedliche Optionen vorgeschlagen:

- Abspaltung von Unternehmensteilen, um dem Geltungsbereich des US-Rechts zu entgehen und somit nicht mehr als Adressat des CLOUD-Acts zu gelten.[1113]
- Implementierung eines Modells einer Datentreuhand durch einen europäischen Dienstleister: der Zugriff auf personenbezogene Daten erfolgt ausschließlich durch den europäischen Dienstleister, während dem US-Recht unterfallenden Verantwortlichen das Verfügungsrecht entzogen ist.[1114] Die personenbezogenen Daten sind dann nicht mehr „im Besitz, Gewahrsam oder unter der Kontrolle“ des vom CLOUD Act Verpflichteten.
- Implementierung einer clientseitigen Verschlüsselung, sodass es schlicht unmöglich ist, unverschlüsselte und damit lesbare Informationen an amerikanische Behörden herauszugeben.[1115]

Nach eigenen Angaben verfolgt der amerikanische KI-System Signal einen entsprechenden Weg die eigenen Zugriffsmöglichkeiten auf Nutzerdaten technisch zu beschränken: auf der eigenen Webseite wird der Fall einer US-behördlichen Anfrage geschildert, welcher der Dienst nicht nachgekommen sei, da die Daten dem Dienstanbieter schlicht nicht vorliegen.[1116] Lediglich das Datum der Erstellung des Accounts und des letzten Zugriffs auf diesen Account sei der Behörde zurückgemeldet worden.[1117] Entscheidend hierbei ist, dass nicht nur (Kommunikationsinhalts-)Daten auf dem Transportweg verschlüsselt werden, sondern auch die Metadaten nicht oder nur in verschlüsselter (und nicht entschlüsselbarer) Form vorliegen.

[1107] Vgl. EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 178 ff.; *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 45 Rn. 24c.

[1108] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 25; *Jansen*, ZD 2018, 149 (150).

[1109] *Gausling*, MMR 2018, 578 (579).

[1110] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 25.

[1111] *European Data Protection Board/European Data Protection Supervisor*, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), S. 8; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 26 ff.

[1112] *Schwartmann/Burkhardt*, ZD 2021, 235 (236).

[1113] *Gausling*, MMR 2018, 578 (582); *Jansen*, ZD 2018, 149 (150).

[1114] *Gausling*, MMR 2018, 578 (582); *Schwartmann/Burkhardt*, ZD 2021, 235 (236). Ein solches Modell haben Microsoft und Deutsche Telekom allerdings bereits wieder beendet: *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 29.

[1115] *Schwartmann/Burkhardt*, ZD 2021, 235 (236).

[1116] Signal, Grand jury subpoena for Signal user data, Central District of California, 27.04.2021, https://signal.org/bigbrother/central-california-grand-jury/: Looking back at how Signal works, as the world moves forward, 05.06.2020, https://signal.org/blog/looking-back-as-the-world-moves-forward/ [letzter Abruf 06.07.2021].

[1117] Signal, Grand jury subpoena for Signal user data, Central District of California, 27.04.2021, https://signal.org/bigbrother/central-california-grand-jury/ [letzter Abruf 06.07.2021].

10.3.3 Zwischenergebnis zum internationalen Datentransfer

Aufgrund der Schutzpflichten der Datenschutzgrundrechte sowie der Gefahr des Unterschreitens eines angemessenen, grundrechtlich gebotenen Datenschutzniveaus durch Übermittlung personenbezogener Daten in Drittstaaten außerhalb des Geltungsbereichs der DSGVO, stellt diese hohe Legitimationsanforderungen an solche Drittstaatentransfers. Der in der Praxis unkomplizierteste Fall – da ohne weitere Genehmigungen oder Prüfungen umsetzbar – ist der Austausch personenbezogener Daten mit Beteiligten in Drittstaaten, für die ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Für andere Drittstaaten eröffnen Standardvertragsklauseln und Binding Corporate Rules Wege für eine Datenübermittlung. Für die USA besteht allerdings insofern erhebliche Rechtsunsicherheit, da unklar ist, wieweit US-amerikanische Unternehmen die notwendigen Klauseln der SCC nach dem zusätzlich für sie maßgeblichen US-amerikanischen Recht einhalten können. Datentransfers als auch Datenzugriffsmöglichkeiten unterliegen in Bezug zu US-amerikanischen Unternehmen daher weiteren Bedingungen, die ein angemessenes Datenschutzniveau sicherstellen und dabei insbesondere behördliche Datenzugriffe ausschließen, die aus EU-rechtlicher Perspektive als unverhältnismäßig eingestuft werden. Welche das konkret sind, um Datenschutzrisiken effektiv zu mitigieren, ist noch Grundlage aktueller Diskussionen. Behalten sich US-amerikanische Unternehmen vor, Datenübermittlungen ohne besondere Sicherheitsvorkehrungen in die USA durchzuführen, bestehen erhebliche Bedenken an einem datenschutzkonformen Einsatz dieser Produkte.[1118] Weitere Ausnahmeregelungen für Drittstaatentransfers sind für den vorliegenden Kontext nur in sehr engen Grenzen einschlägig. Insbesondere die Einwilligung als Legitimationsgrundlage dürfte im Beschäftigtenkontext mangels Freiwilligkeit regelmäßig ausscheiden. Achtung ist auch dann geboten, wenn Anbieter zwar selbst in der EU/EWR verortet sind, aber Unterauftragnehmer aus den USA zum Einsatz kommen.[1119]

10.4 Besonderheiten der elektronischen Kommunikation

KI-Systeme können auch im Bereichen zum Einsatz kommen, welche zur elektronischen Kommunikation gezählt werden. So sind KI-gestützte Chat-Bots klassische Beispiele, welche mit natürlichen Personen über Fernkommunikationsmittel interagieren und dabei sowohl im Hinblick auf die Kommunikationsinhalte als auch die Kommunikationsmetadaten regelmäßig personenbezogene Daten anfallen können.

Der Bereich der elektronischen Kommunikation wird von der ePrivacy-Richtlinie erfasst, diese bedarf allerdings der Umsetzung in mitgliedstaatliches Recht. Im Frühjahr 2021 wurden diese Umsetzungsrechtsakte im TTDSG und TKModG novelliert. Damit wurden die bisherigen datenschutzrechtlichen Regelungen in TKG a.F. und TMG a.F. in einem gemeinsamen Gesetz zusammengeführt. Teil 2 des TTDSG widmet sich der Telekommunikation, während Teil 3 eher Telemedien adressiert. Allerdings wird es sich dabei voraussichtlich nur um eine Zwischenlösung handeln, da der Plan einer unmittelbar geltenden ePrivacy-Verordnung noch nicht aufgegeben wurde.

[1118] *Schwartmann/Burkhardt*, ZD 2021, 235 (237).
[1119] *Rohrlich*, ZAP 2020, 1265 (1270).

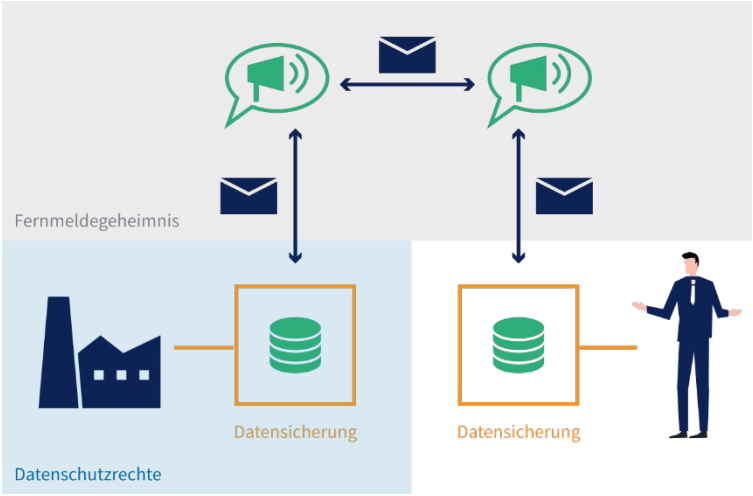


Abbildung 23 Schutzbereich des Fernmeldegeheimnisses

10.4.1 Rollenkonzept

Das TTDSG adressiert nicht nur die Verarbeitung personenbezogener Daten, sondern geht darüber hinaus.[1120] Insofern werden auch nicht die Begriffe des Verantwortlichen und der betroffenen Personen als zentrale Rollen benannt, sondern die Anbieter und Nutzer.

Anbieter von Telemedien: sind gemäß § 2 Abs. 2 Nr. 1 TTDSG jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt.

Anbieter von Telekommunikationsdiensten: Das TTDSG selbst enthält keine Definition des TK-Dienstes. Dieses findet sich im TKG. Nach § 3 Nr. 1 i.V.m. Nr. 61 TKG sind Anbieter von Telekommunikationsdiensten: „jeder, der Telekommunikationsdienste erbringt". Dabei handelt es sich um in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:

a) Internetzugangsdienste,

b) interpersonelle Telekommunikationsdienste[1121] und

c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.

Endnutzer: Nach § 3 Nr. 13 TKG ist „Endnutzer" ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt. Das TMG definiert den „Nutzer" in

[1120] Vgl. *DSK - Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), S. 5.

[1121] „Interpersoneller Telekommunikationsdienst" ist gemäß § 3 Nr. 24 TKG ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen.

§ 2 S. 1 Nr. 3 TMG als jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

10.4.2 Telekommunikation

Verpflichtet werden:

- Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie an der Diensterbringung Mitwirkende,
- Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie an der Diensterbringung Mitwirkende,
- Betreiber öffentlicher Telekommunikationsnetze und
- Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.

Im Hinblick auf das Zusammenspiel zwischen DSGVO und der ePrivacy-Richtlinie, welches in Art. 95 DSGVO geregelt ist, gilt allerdings zu bedenken, dass der Anwendungsvorrang der DSGVO nur für den Bereich der Datenverarbeitung in Verbindung mit der Bereitstellung *öffentlich zugänglicher* elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen zurückgenommen wird.[1122] Insofern dürfte die Ausweitung auf lediglich *geschäftsmäßig* angebotene Telekommunikationsdienste den Regelungsspielraum des deutschen Gesetzgebers überschreiten, sofern dieses Angebot nicht öffentlich ist, bspw. bei betriebsinternen Kommunikationslösungen.[1123]

Verarbeitung von Verkehrsdaten: § 3 Nr. 70 TKG definiert Verkehrsdaten allgemein als „Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind“. Nach § 9 Abs. 1 TTDSG dürfen bestimmte Verkehrsdaten, wozu u.a. Anschlussnummer, Verbindungsdaten, Entgelte und Datenmengen sowie sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendigen Daten zählen (§ 9 Abs. 1 S. 1 Nr. 1-5 TTDSG), verarbeitet werden, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind sie nach Beendigung der Verbindung unverzüglich zu löschen. Darüber hinaus gehende Verarbeitungen bedürfen der Einwilligung (§ 9 Abs. 2 TTDSG). Daten anderer Endnutzer sind unverzüglich zu anonymisieren.

Entgeltermittlung und Entgeltabrechnung § 10 TTDSG regelt nochmals spezifischer die Datenverarbeitung zu Abrechnungszwecken.

Einzelverbindungsnachweis Die Regelung des § 11 TTDSG betrifft die besondere Form der Abrechnung von Telekommunikationsdienstleistungen, indem die Rechnung nach Einzelverbindungen aufgeschlüsselt wird.

Störungen und Missbrauch von Telekommunikationsanlagen und -diensten § 12 TTDSG regelt Anforderungen an die Erkennung, Eingrenzung und Beseitigung von Störungen und Fehlern (Abs. 1–2), das Aufschalten auf bestehende Verbindungen (Abs. 3) und das Aufdecken und Unterbinden von rechtswidrigen Inanspruchnahmen von Telekommunikationsnetzen und -diensten (Abs. 4).

[1122] *Holländer,* in: BeckOK DatenschutzR Art. 95 Rn. 4; *Kühling/Raab,* in: Kühling/Buchner - DS-GVO/BDSG Art. 95 Rn. 11; *Sydow*, Sydow, Europäische Datenschutzgrundverordnung Art. 95 Rn. 10; *Golland,* in: Taeger/Gabel - DSGVO/BDSG Art. 95 Rn. 17.

[1123] *Wagner u. a.*, Daten- und Geheimnisschutz bei der Kommunikation im Unternehmenskontext, S. 145 ff. m.w.N.

Standortdaten § 13 TTDSG regelt die Nutzung von Standortdaten zur Bereitstellung von *Diensten mit Zusatznutzen*.[1124] Damit soll die Nutzung von Telekommunikationsdiensten standortbezogen ermöglicht werden (Location-Based-Services, LBS wie bspw. Navigationsdienste, Informationen zu Einrichtungen vor Ort, ortsgebundene Werbung etc).[1125] Gleichzeitig werden Standortdaten als besonders schutzwürdige Daten eingeordnet, weil das Wissen um Aufenthaltsorte und -zeiten sowie Möglichkeiten zur Erstellung von Bewegungsprofilen umfangreiche Rückschlüsse auf Lebensgewohnheiten und die Persönlichkeit der Betroffenen ermöglicht.[1126] Das TKG definiert Standortdaten als:

> **§ 3 Nr. 56 TKG** „Standortdaten" Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben

Diese dürfen nur im erforderlichen Umfang und erforderlichen Zeitraum verarbeitet werden, sofern sie anonymisiert wurden oder die Nutzer*in eingewilligt hat. Voraussetzungen sin somit:

- Zur Bereitstellung eines **Dienstes mit Zusatznutzen**
- **Erforderlichkeit** im Hinblick auf Umfang und Dauer der Datenverarbeitung
- Legitimation durch:
  - **Anonymisierung** oder
  - **Einwilligung**

Aus der Formulierung wird von *Munz* geschlussfolgert, dass selbst wenn es sich um anonyme Daten handelt – womit normalerweise der datenschutzrechtliche Schutzanspruch endet – eine Verarbeitung nur im engen Rahmen des § 13 TTDSG zulässig sein soll.[1127] Die Information der Endnutzer*in über die Standorterhebung hat über Textmitteilung an das Endgerät zu erfolgen, es sei denn der Standort wird nur auf dem Endgerät angezeigt, dessen Standortdaten ermittelt wurden. Die Weitergabe von Strandortdaten an Dritte erfordert eine ausdrücklich, gesondert und schriftlich erteilte Einwilligung (Fremdortung). Das Recht, die Anzeige von Daten zu unterdrücken, bleibt unberührt.[1128] Für Notrufnummern 112 oder 110 oder den Rufnummern 124 124 oder 116 117 soll hingegen sichergestellt werden, dass die Übermittlung von Standortdaten nicht dauernd ausgeschlossen wird. Hier bedarf die Standortermittlung nicht der Einwilligung, da ein Einwilligungserfordernis das Anliegen, Rettungsdiensten schnelle und effektive Hilfeleistungen zu ermöglichen, gefährden könnte.[1129]

10.4.3 Telemedien

Die Regelungen im 3. Teil des TTDSG richten sich an Anbieter von Telemedien. Dies sind gemäß § 2 Abs. 2 Nr.

[1124] Definiert in § 2 Abs. 2 Nr. 5 TTDSG als „jeder von einem Anbieter eines Telekommunikationsdienstes bereitgehaltene zusätzliche Dienst, der die Verarbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder für die Entgeltabrechnung des Telekommunikationsdienstes erforderliche Maß hinausgeht".
[1125] *Munz,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 13 TTDSG Rn. 1.; *Tinnefeld/Buchner,* in: BeckOK DatenschutzR, Kap. Syst. I. Datenschutz in Medien und Telekommunikation Rn. 130.
[1126] *Tinnefeld/Buchner,* in: BeckOK DatenschutzR, Kap. Syst. I. Datenschutz in Medien und Telekommunikation Rn. 128.
[1127] *Munz,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 13 TTDSG Rn. 11.
[1128] BT-Drs. 15/2316, S. 89.
[1129] *Munz,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 13 TTDSG Rn. 21.

1 TTDSG „jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt." Telemedien sind nach der Legaldefinition des § 1 Abs. 1 TMG:

> **alle elektronischen Informations- und Kommunikationsdienste,** soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 61 TKG, telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG oder Rundfunk nach § 2 Rundfunkstaatsvertrag sind

Das Verhältnis der telemedienspezifischen Regelung zu anderen gesetzlichen Vorschriften bleibt an vielen Stellen unklar, weil die Vorgaben weitestgehend unreflektiert aus den Vorgängernormen übernommen wurden.[1130] Sofern Überschneidungen zur DSGVO bestehen, welche nicht im Regelungsbereich der ePrivacy-Richtlinie liegen, besteht weiterhin die Problematik, dass es außerhalb expliziter Öffnungsklauseln zu einer Unanwendbarkeit bestimmter Vorgaben kommen kann.[1131]

Technische und organisatorische Vorkehrungen: § 19 TTDSG adressiert folgende Aspekte:

- Jederzeitige Möglichkeit die Dienstnutzung zu beenden
- Telemediennutzung geschützt gegen Kenntnisnahme Dritter
- Ermöglichung der Telemediennutzung und Bezahlung anonym oder unter Pseudonym, soweit dies technisch möglich und zumutbar ist
- Anzeige bei Weitervermittlung zu einem anderen Anbieter
- Für *geschäftsmäßig*[1132] angebotene Telemedien im Rahmen der technischen Möglichkeit und wirtschaftlichen Zumutbarkeit Einsatz von TOMs unter Berücksichtigung des Stands der Technik, die sicherstellen, dass
  - kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
  - diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

Verarbeitung personenbezogener Daten Minderjähriger: § 20 TTDSG enthält ein Kommerzialisierungsverbot von Daten Minderjähriger, die der Anbieter zur Wahrung des Jugendschutzes, bspw. zur Altersverifikation, erhoben hat.

Bestandsdaten: Gegenstand von § 21 TTDSG ist die Bestandsdatenauskunft zum Zweck der Durchsetzung bestimmter zivilrechtlicher Ansprüche.[1133] Bestandsdaten sind gemäß § 2 Abs. 2 Nr. 2 TTDSG personenbezogenen Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter von Telemedien und dem Nutzer über die Nutzung von Telemedien erforderlich ist.

Schutz der Privatsphäre bei Endeinrichtungen: Die besser als „Cookie-Regelung" bekannte Norm des § 25 TTDSG macht die Speicherung von Informationen auf Endeinrichtungen und den Zugriff auf bereits dort gespeicherte Informationen von einer Einwilligung des Endnutzers abhängig. Endeinrichtung ist in § 2 Abs. 2 Nr. 6 TTDSG definiert

---

[1130] So auch: *Moos,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 19 TTDSG Rn. 3.
[1131] *Moos,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 19 TTDSG Rn. 3.
[1132] Laut Gesetzesbegründung, wenn es „auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt" BT-Drs. 18/4096, S. 34. Somit wird das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine nicht erfasst. *Moos,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 19 TTDSG Rn. 31.
[1133] *Ettig,* in: Taeger/Gabel, DSGVO - BDSG - TTDSG, § 21 TTDSG Rn. 1.

> jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet.

Auch vernetzte Geräte (IoT) und vernetzte Fahrzeuge fallen unter die Endeinrichtungen.[1134] Die Norm erfasst sowohl personenbezogene als auch nicht-personenbezogene Daten.[1135] Somit sollen bspw. auch Updates darunter fallen.[1136] Ausnahmen gelten nach Abs. 2, wenn:

- der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist, oder
- die Handlung unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Einwilligungsverwaltung: Da die Umsetzung der persönlichen Datenschutzpräferenzen oftmals an Hürden, wie Nudging, Deep Patterns oder dem Aufwand individuelle Einstellungen vorzunehmen, scheitern, versprechen sog. Personal Information Management Systems (PIMS) einen nutzerfreundlicheren Datenschutz, indem sie eine digitale Einwilligungsassistenz bieten. Ein Gedanke dabei ist, dass Nutzer*innen ihre Datenschutzpräferenzen abstrakt-generell festlegen und das PIMS im konkreten Einzelfall die Einwilligung automatisiert erklärt.[1137] § 26 TTDSG soll in Kombination mit einer die Anforderungen konkretisierenden Rechtsverordnung einen Rechtsrahmen für PIMS im Hinblick auf die Einwilligungen nach § 25 TTDSG schaffen. Allerdings bleibt zu diskutieren, ob automatische Assistenzsysteme die Anforderungen der DSGVO an eine wirksame Einwilligung erfüllen.[1138] Bei der rein automatisierten Übermittlung bereits zuvor durch die betroffene Person gewählter Einstellungsparameter bestehen hierzu erheblich weniger Bedenken, als wenn das PIMS-System autonom abstrakt-generelle Präferenzen in konkrete Entscheidungen übersetzen muss.[1139]

10.5 Zwischenergebnis zu kontextspezifischen Datenschutzanforderungen und KI

Da KI-Systeme grundsätzlich in unterschiedlichsten Szenarien zum Einsatz kommen können, sollte mitbedacht werden, ob kontextspezifische oder sektorspezifische Datenschutzregelungen einschlägig sind. Besonders hohe Anforderungen bestehen bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Auch im Hinblick auf Datentransfers in Drittländer sind nochmals Grenzen gesetzt.

Der Bereich der elektronischen Kommunikation wurde jüngst im TTDSG neu aufgelegt – dies dürfte allerdings nur eine Zwischenlösung darstellen, bis auf EU-Ebene die ePrivacy-Verordnung erlassen wird.

[1134] *DSK - Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), S. 7.
[1135] *DSK - Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), S. 7.
[1136] *DSK - Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), S. 7.
[1137] *Botta*, MMR 2021, 946 (946).
[1138] *Botta*, MMR 2021, 946 (948 ff.).
[1139] *Botta*, MMR 2021, 946 (948).

— Anhänge

Glossar und Abkürzungsverzeichnis

Abkürzungen

a. A.	Andere Ansicht
a. F.	Alte Fassung
Abs.	Absatz
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
APR	Allgemeines Persönlichkeitsrecht
ArbG	Arbeitsgericht
Art.	Artikel
AV	Auftragsverarbeitung
AV-Vertrag	Auftragsverarbeitungsvertrag
BAG	Bundesarbeitsgericht
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BImschG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
CMS	Compliance-Management-Systeme
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung VO (EU) 2016/679
DSK	Datenschutzkonferenz (Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden

	des Bundes und der Länder)
DSMS	Datenschutzmanagementsysteme
EDSB / EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA / EDPB	Europäischer Datenschutzausschuss / European Data Protection Board (vormals Art-29-Datenschutzgruppe)
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EWR	Europäischer Wirtschaftsraum
ePrivacy-RL	Datenschutzrichtlinie für elektronische Kommunikation, Richtlinie 2002/58/EG
ePrivacy-VO	Geplante Verordnung zur Ablösung der ePrivacy-RL
EuGH	Europäischer Gerichtshof
EU-GrCh	EU-Grundrechtecharta
f.	folgende (die folgende Seite/der folgende Paragraph/Artikel/etc.)
ff.	fortfolgende (mehrere folgende Seiten/Paragraphen/Artikel/etc.)
GG	Grundgesetz
HGB	Handelsgesetzbuch
ISMS	Information Security Management Systems
KG	Kammergericht
KI	Künstliche Intelligenz
KI-VOE	KI-Verordnungsentwurf
LAG	Landesarbeitsgericht
LDSG	Landesdatenschutzgesetz
LfDI	Landesbeauftragte für den Datenschutz und die Informationsfreiheit
LG	Landgericht
m. w. N.	Mit weiteren Nachweisen
n. F.	Neue Fassung
OLG	Oberlandesgericht
PIMS	Personal Information Management Systems
RL	Richtlinie
Rn.	Randnummer
SCC	Standard Contractual Clauses / Standardvertragsklauseln
SDM	Standard-Datenschutzmodell
Sog.	sogenannt
TK-Dienst	Telekommunikationsdienst
TKG	Telekommunikationsgesetz

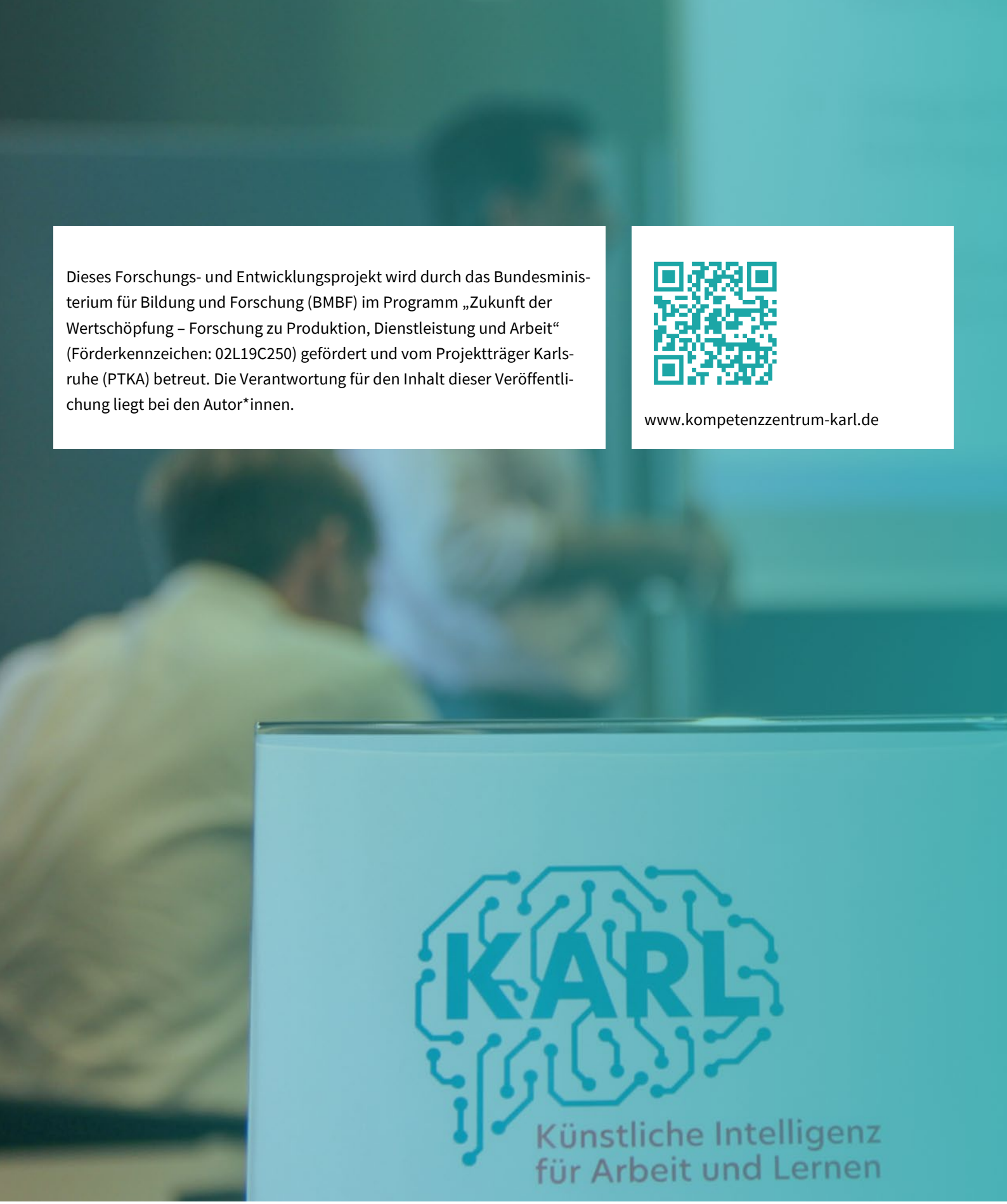
TMG	Telemediengesetz
TOM	Technische und organisatorische Maßnahmen
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
Vgl.	Vergleiche
VO	Verordnung
VwVfG	Verwaltungsverfahrensgesetz
XAI	Explainable Artificial Intelligence

Glossar zu verwendeten Begriffen

Auftragsverarbeiter	Im Auftrag eines Verantwortlichen tätige Stelle definiert in Art. 4 Nr. 8 DSGVO, die keine eigenen Verarbeitungszwecke verfolgt
Autonomie	Zustand der Selbstbestimmung, Unabhängigkeit (Souveränität) oder Entscheidungs- bzw. Handlungsfreiheit
Beschäftigte	Arbeitnehmer*innen / Mitarbeiter*innen eines Unternehmens / Organisation, definiert in § 26 Abs. 8 BDSG
Besondere Kategorien personenbezogener Daten	Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person i.S.d. Art. 9 Abs. 1 DSGVO
Betroffene Person	Identifizierte oder identifizierbare natürliche Person, auf die sich Daten beziehen i.S.d. Art. 4 Nr. 1 DSGVO
Betroffenenrechte	Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung bzw. Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch und Ausschluss automatisierter Entscheidungen im Einzelfall (Kapitel 3 DSGVO)
Daten	Informationen (hier Synonym verwendet)
Datenschutzgrundrechte	Bezieht sich auf die datenschutzrechtlich relevanten Grundrechte wie Recht auf informationelle Selbstbestimmung, Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme, Achtung des Privat und Familienlebens, Recht auf Schutz personenbezogener Daten
Drittstaat / Drittland	Staat bzw. Land außerhalb der EU und des EWR
KI-System	System, dass in der Lage zu eigenständigen Verhaltensweisen bzw. Entscheidungsfindung ist, über Prognosefähigkeit oder die Fähigkeit zu autonomen Lern- und Adaptionsprozessen verfügt.

Neuronale Netze	Künstliche neuronale Netze sind vernetzte Neuronen, welche biologischen Vorbilden nachgebildet sind, um zu „lernen“.
Privacy by Default	Datenschutzfreundliche Voreinstellungen (vgl. Art. 25 Abs. 2 DSGVO)
Privacy by Design	Datenschutzfreundliche Technikgestaltung (vgl. Art. 25 Abs. 1 DSGVO)
Testdaten	Datensatz, der nicht mit Trainingsdaten identisch ist, um die Qualität eines trainierten Modells zu überprüfen.
Trainingsdaten	Datensatz, der zum Lernen von Mustern und Zusammenhängen genutzt wird.
Transparenz	Nachvollziehbarkeit von Vorgängen
Unternehmen	Wirtschaftlich selbstständige Organisationseinheit, wobei im vorliegenden Kontext privatrechtlich organisierte Unternehmen im Fokus stehen. Hierbei handelt es sich regelmäßig um juristische Personen oder Personengesellschaften (z.B. GmbH, AG, SE etc.)
Validierungsdaten	Datensatz für die Abstimmung der Parameter eines KI-Systems.
Verantwortlicher	Für die Verarbeitung personenbezogener Daten verantwortliche Stelle definiert in Art. 4 Nr. 7 DSGVO

DOI: 10.5445/IR/1000161675



Dieses Forschungs- und Entwicklungsprojekt wird durch das Bundesministerium für Bildung und Forschung (BMBF) im Programm „Zukunft der Wertschöpfung – Forschung zu Produktion, Dienstleistung und Arbeit“ (Förderkennzeichen: 02L19C250) gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autor*innen.

www.kompetenzzentrum-karl.de

KARL
Künstliche Intelligenz
für Arbeit und Lernen

Kompetenzzentren
Arbeitsforschung

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung