Künstliche Intelligenz & Datenschutz

Praxisleitfaden Version 2.0 | Neuauflage

bitkom

Inhalt

Geleitwort

Der vorliegende Leitfaden wurde federführend von den Mitgliedern des Arbeitskreises Datenschutz des Bitkom erstellt. Besonderer Dank gilt den folgenden Autorinnen und Autoren, die sich mit viel Mühe und Hingabe der Erstellung des Leitfadens gewidmet haben:

- Dr. Christoph Bausewein, CrowdStrike GmBH
- Daniel Beise, freenet DLS GmbH
- Dr. Alexander Fritz, OmegaLambdaTec GmbH
- Ralf Herter, BASF SE
- Susan Hillert, Taylor Wessing Partnerschaftgesellschaft mbB
- Anja Hillig, WIPIT Partnerschaft mbB Rechtsanwälte Steuerberater
- Alexander Höcht, Fujitsu
- Petra Möritz, DATEV eG
- Paul Pink, DHL Group
- René Schneider, IPAI Aleph Alpha Research GmbH
- Sophie Sohm, Meta Group Germany GmbH
- Susanna Wolf, DATEV eG

Wir bedanken uns ebenfalls bei den Autorinnen und Autoren, die an der Vorgängerversion des Leitfadens mitgewirkt haben.

Stefanie Bauer, ePrivacy GmbH | Arnd Böken, GvW Graf von Westphalen Rechtsanwälte Steuerberater Partnerschaft mbB | Dr. Nadja Christe, Bayer AG | Jonas von Dall'Armi, Giesecke+Devrient GmbH | Nils Freymuth, MSD Sharp & Dohme GmbH | Markus Frowein, RWE AG | Dr. Inka Knappertsbusch, LL.M., CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB | Stefan Mangold, DATEV eG | Tobias Messerschmidt, DHL Group | Dirk Refflinghaus, Finanz Informatik GmbH & Co. KG | Janine Richter, BREDEX GmbH | Lys Riemenschneider, Holisticon AG | Jens Schreiber, medatixx GmbH & Co. KG | Dr. iur. Dr. rer. pol. Hans Steege, CARIAD SE | Florian Thoma, Accenture | Jörn Wittmann, Volkswagen AG

Ziel dieses Projektes ist es, das Spannungsverhältnis zwischen Künstlicher Intelligenz (KI) und Datenschutz sowohl in einer verständlichen als auch in einer fachlich anspruchsvollen Art und Weise darzustellen und konkrete Handlungsempfehlungen zu geben. Es ist unser Bestreben, dieses Dokument kontinuierlich zu überarbeiten und zu aktualisieren, um den neuesten Entwicklungen auf dem Gebiet von KI und Datenschutz Rechnung zu tragen. Wir laden daher alle Interessierten herzlich ein, sich aktiv an der Weiterentwicklung des Leitfadens zu beteiligen.

1 Ziel des Leitfadens

Der »KI & Datenschutz Praxisleitfaden« unterstützt Unternehmen und Organisationen dabei, Künstliche Intelligenz (KI) datenschutzkonform einzusetzen. Ziel ist es, konkrete Handlungsempfehlungen und rechtliche Orientierung bereitzustellen, damit der Umgang mit personenbezogenen Daten im Einklang mit der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) (DS-GVO) sowie weiteren einschlägigen Regelwerken erfolgt.

Der Leitfaden richtet sich insbesondere an Datenschutzbeauftragte, IT- und Compliance-Verantwortliche, Entwicklerinnen und Entwickler sowie Anwenderinnen und Anwender von KI-Systemen – ebenso wie an Entscheidungsträgerinnen und Entscheidungsträger, die für die strategische Ausrichtung von KI-Projekten verantwortlich sind.

Während sich unser Leitfaden »Generative KI im Unternehmen« mit den allgemeinen Aspekten und Rahmenbedingungen der Nutzung von generativer KI beschäftigt, konzentriert sich dieser Praxisleitfaden speziell auf die datenschutzrechtlichen Anforderungen und ethischen Überlegungen bei der Nutzung von KI-Technologien.

Er bietet detaillierte, praxisnahe Anleitungen und Beispiele, die speziell auf die datenschutzkonforme Implementierung von KI-Anwendungen abzielen.

Durch präzise Definitionen, praxisorientierte Checklisten und verständlich aufbereitete rechtliche Grundlagen schafft der Leitfaden Klarheit im Umgang mit datenschutz-rechtlichen Herausforderungen. Dabei ergänzt er den bestehenden Leitfaden »Generative KI im Unternehmen«, der sich auf die allgemeinen Rahmenbedingungen und Nutzungsmöglichkeiten generativer KI konzentriert. Im Fokus dieses Leitfadens stehen hingegen die datenschutzrechtlichen Anforderungen und ethischen Implikationen beim Einsatz von KI-Technologien.

Der Aufbau des Leitfadens ist bewusst praxisnah gewählt:

Zu Beginn werden grundlegende Fragestellungen behandelt: Was verstehen wir unter KI? Welche ethischen Aspekte gilt es zu beachten? Und welche rechtlichen Rahmen-bedingungen greifen beim KI-Einsatz?

Anders als in der Vorgängerversion haben wir die Checkliste, welche zentrale Maßnahmen für den datenschutzkonformen Einsatz von KI darstellt, in den zweiten Abschnitt gezogen. So soll Leserinnen und Lesern direkt zu Beginn ein Überblick über die zu prüfenden Punkte gegeben werden.

Im dritten Abschnitt folgen konkrete Anforderungen der DS-GVO in Bezug auf KI – ergänzt durch Hinweise zur Erstellung von internen Richtlinien, Lösch- und Berechtigungskonzepten.

Dieser Leitfaden bietet somit einen praktischen Werkzeugkasten für alle, die KI-Technologien rechtssicher und verantwortungsvoll in ihrer Organisation etablieren möchten.

Wann sprechen wir überhaupt von Künstlicher Intelligenz?

Der Begriff »Künstliche Intelligenz« (KI) wird in öffentlichen Debatten, der Unternehmenspraxis und nicht zuletzt im Marketing regelrecht inflationär verwendet – oftmals ohne genaue Definition oder technisches Verständnis. Viele Anwendungen, die als »KI« etikettiert werden, sind in Wirklichkeit bloße automatisierte, regelbasierte Systeme oder Formen von maschinellem Lernen mit sehr spezifischem Einsatzzweck. Für Unternehmen, die den rechtskonformen Einsatz von KI-Systemen sicherstellen wollen, ist deshalb ein differenzierter, kritischer und zugleich praxisnaher Blick auf den Begriff unerlässlich.

Der Begriff stammt aus der Informatik, wo KI ursprünglich als Versuch verstanden wurde, kognitive Fähigkeiten des Menschen – wie Lernen, Problemlösen oder Sprachverstehen – durch Maschinen zu simulieren. Diese Vorstellung ist bis heute prägend, jedoch missverständlich: Aktuelle KI-Systeme verfügen nicht über Bewusstsein, Selbstreflexion oder ein eigenständiges Verständnis der Welt. Sie sind nicht »intelligent« im menschlichen Sinne. Vielmehr handelt es sich um von Menschen entwickelte und mit gewaltiger Rechenleistung trainierte Systeme, die durch statistische Methoden Muster in Daten erkennen, Wahrscheinlichkeiten berechnen oder auf Basis expliziter Regeln, Zielvorgaben oder durch Belohnungsmechanismen Inhalte erzeugen.

Berechtigterweise wird daher häufig von Experten wie Kate Crawford (Atlas der KI, C.H. Beck Verlag, 2024) gemahnt, dass KI weder »künstlich« noch »intelligent« ist, sondern das Produkt eines komplexen sozialen, technischen und wirtschaftlichen Gefüges – ein »Register der Macht«, das nicht neutral ist, sondern bestehende Strukturen spiegeln und verstärken kann. Sie und andere kritisieren zu Recht, dass KI in der Praxis häufig als Blackbox verstanden wird, obwohl es sich um von Menschen entwickelte und betriebene Systeme handelt, die auf Ressourcen, menschliche Arbeit und politische wie infrastrukturelle Voraussetzungen angewiesen sind.

Die EU-KI-Verordnung (Verordnung (EU) 2024/1689) (KI-VO) ist ein Beispiel dafür, die hinsichtlich »KI« von einem »maschinengestützten System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist, […] und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt […]« spricht. Das kann viele Formen annehmen – von Chatbots über Empfehlungssysteme bis hin zu komplexen Steuerungs- und Überwachungssystemen in kritischer Infrastruktur.

Insofern gilt: Nicht jede Form von Automatisierung oder maschinellem Lernen (ML) ist gleich »KI« im Sinne der Verordnung. Viele Systeme – etwa regelbasierte Programme oder einfache datengetriebene Analysen – fallen nicht unter das KI-Regime. Erst wenn bestimmte Kriterien erfüllt sind, etwa Lern- und Anpassungsfähigkeit, Entscheidungsautonomie und ein potentielles Risiko für Sicherheit, Gesundheit oder Grundrechte, greift die KI-VO. Damit wird deutlich: Der Begriff »KI« darf nicht pauschalisiert, sondern muss im jeweiligen Kontext bewertet werden.

Beispiele:

1. **Excel-Auswertung: keine KI im Sinne der KI-VO**
   Ein Unternehmen nutzt Microsoft Excel, um Verkaufszahlen zu analysieren – z. B. mit Pivot-Tabellen, Formeln oder Balkendiagrammen. Die Regeln sind manuell definiert, es findet kein Lernen oder Anpassen statt. Es handelt sich um regelbasierte Datenverarbeitung ohne Lernfähigkeit oder autonome Entscheidungsfindung und fällt daher nicht unter den Anwendungsbereich der KI-VO.

2. **Im Unternehmen eingesetzte Chatbots**
   Unternehmen setzen auf ihren Webseiten Chatbots ein, die auf Grundlage vorab definierter Anweisungen und eines trainierten KI-Modells automatisch Textinhalte generieren – z. B. zur Beantwortung häufig gestellter Fragen im Kundenservice. Solche Systeme fallen unter den Anwendungsbereich der KI-Verordnung, da sie auf einem vortrainierten Modell basieren und eine gewisse Entscheidungsautonomie aufweisen. Je nach Einsatzbereich – etwa im Gesundheits-, Finanz- oder Bildungswesen – können sie als Hochrisiko-KI-Systeme im Sinne des Art.6 KI-VO eingestuft werden, sofern ein erhebliches Risiko für Grundrechte, Sicherheit oder Gesundheit besteht.

3. **GPAI-Modelle (Generative KI mit allgemeinem Verwendungszweck)**
   Hier geht es um KI-Modelle mit allgemeinem Verwendungszweck, wie z. B. ChatGPT von OpenAI, die mit riesigen Datenmengen trainiert werden. GPAI-Modelle werden im Art.3 Nr. 63 der KI-VO definiert und unterliegen besonderen Anforderungen.

Für die betriebliche Praxis bedeutet das:

- Begriffspräzision ist essenziell. Nicht alles, was automatisiert oder lernfähig ist, ist gleich KI im rechtlichen Sinne.
- Kritisches Bewusstsein ist notwendig. Systeme sollten nicht unreflektiert als »intelligent« bezeichnet oder mit menschlichen Fähigkeiten gleichgesetzt werden.
- Rechtskonformität muss kontextbezogen geprüft werden. Die Einordnung eines Systems als KI im Sinne der KI-Verordnung hängt von technischen Merkmalen und dem konkreten Einsatzkontext ab.

Zugleich erfordert ein konstruktiver Umgang mit KI keine Angst, sondern Aufgeschlossenheit und Klarheit: Wo die Technik sinnvoll eingesetzt wird, kann sie Effizienz steigern und neue Erkenntnisse ermöglichen – vorausgesetzt, Unternehmen berücksichtigen dabei sowohl die Vorgaben der DS-GVO als auch die Anforderungen der KI-VO.

Nur wer versteht, was KI ist – und was nicht, kann den tatsächlichen Risiken mit Augenmaß begegnen und die Chancen verantwortungsvoll nutzen.

Ethischer Rahmen: Vertrauenswürdige KI-Gestaltung strategisch verankern und umsetzen

Der mit dem zunehmenden Einsatz von KI verbundene Fortschritt bringt auch Herausforderungen mit sich, insbesondere im Hinblick auf einen vertrauenswürdigen KI-Einsatz. Inwieweit hierbei ethische Kriterien mit Blick auf die bestehende Regulatorik zum Tragen kommen und welche Rolle die Verantwortung von Unternehmen in diesem Zusammenhang spielt, behandelt der folgende Abschnitt.

Bei der ethischen Bewertung von KI-Produkten ist eine wertorientierte Technologiegestaltung entscheidend. Die Werte, die hierbei berücksichtigt werden sollten,

hängen vom Einsatzkontext ab. Dabei ist zu beachten, dass auch die KI-VO eine klare wertebasierte Ausrichtung verfolgt. Besonders hervorgehoben werden dabei die Prinzipien Transparenz, Fairness und menschliche Aufsicht (Human Oversight). Ergänzend rückt zunehmend auch der Wert der Partnerschaftlichkeit in den Fokus einer verantwortungsvollen KI-Gestaltung. Ein mögliches Vorgehen zur Umsetzung dieses Wertes ist die Pilotierung des KI-Produkts mit einer repräsentativen Gruppe von Stakeholdern. Dabei sollten nicht nur Usability-Aspekte, sondern insbesondere der Dialog mit den Beteiligten über ihre Perspektiven auf den Technologieeinsatz sowie über wahrgenommene Chancen und Herausforderungen im Vordergrund stehen. Grundsätzliche Werte können in Codes of Conduct oder vergleichbaren Kodizes von Unternehmen und Institutionen festgehalten sein. Es existieren verschiedene Ansätze für die ethische Bewertung von KI.

Beispiele hierfür sind:

- der Responsibility-Aspekt in der ISO/IEC 42001 (Managementsystemnorm für KI)
- die Werte der High-Level Expert Group on AI (HLE) der EU-Kommission[1]
- die Stellungnahme des deutschen Ethikrats
- die OECD-Prinzipien für vertrauenswürdige KI oder
- die im Rahmen der VDE SPEC 90012 vergleichend gesichteten Leitlinien.

Ein wichtiger Wert bei der Entwicklung und dem Betrieb von KI ist Transparenz.

Hierbei sollten die Funktionen und Verarbeitungsmethoden der KI-Systeme mindestens für die relevanten Zielgruppen angemessen offen und verständlich sein, um das sogenannte Blackbox-Phänomen zu vermeiden.

Bei der Fairness von KI-Anwendungen sollte bereits bei der Entwicklung auf nicht intendierten Bias geachtet werden, um Verzerrungen in den Ergebnissen und Diskriminierung zu vermeiden. Stattdessen sollten KI-Anwendungen Vielfalt und Chancengleichheit fördern. Ein prägnantes Beispiel für potenziellen Bias ist der Einsatz von KI-Systemen im Personalwesen. Werden solche Systeme mit historischen

[1] EU-Kommission, High Level Expert Group on Artificial Intelligence, Ethics Guidelines for trustworthy AI, 08.04.2019. abrufbar unter: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf (zuletzt abgerufen am 23.05.2025).

Lebensläufen trainiert, die stereotype Muster enthalten, kann dies dazu führen, dass bestimmte Gruppen bei der Bewerberauswahl benachteiligt werden.

Darüber hinaus kann der sogenannte »Automation Bias« die Wahrnehmung von KI-Ergebnissen beeinflussen. Dabei neigen Nutzer dazu, automatisierten Entscheidungen übermäßig zu vertrauen, selbst wenn diese fehlerhaft sind. Dies ist besonders relevant bei generativen KI-Modellen (GenAI) und großen Sprachmodellen (LLMs), deren Ausgaben oft als objektiv wahrgenommen werden, obwohl sie auf fehlerhaften oder voreingenommenen Trainingsdaten basieren können.

Studien unterstreichen die Bedeutung dieser Aspekte. Eine Untersuchung des TÜV-Verbands aus dem Jahr 2022 ergab, dass 66 Prozent der Befragten die Gefahr sehen, durch automatisierte Entscheidungen diskriminiert oder benachteiligt zu werden. Als Ursachen wurden unter anderem unzureichende Trainingsdaten und unbedachte Programmierung genannt.[2]

Insgesamt sollten ethische Kriterien in der KI-Entwicklung und im KI-Betrieb zu einem ganzheitlichen Risikomanagement beitragen, zentrale demokratische Werte wahren und deren Operationalisierung nachvollziehbar gestalten. Die Auseinandersetzung mit ethischen Anforderungen dient dabei nicht nur dem betriebswirtschaftlichen Erfolg, etwa durch gesteigertes Vertrauen von Stakeholdern, höherer Akzeptanz bei Mitarbeitenden oder verbesserten Recruiting-Chancen. Gerade im Bereich Fairness trägt sie auch wesentlich zum Schutz von Grundrechten bei und fördert einen nachhaltigen, gesellschaftlich akzeptierten Einsatz von KI-Anwendungen.

Rechtsrahmen beim Einsatz von KI

Für Unternehmen ist der Einsatz von KI mit erheblichen rechtlichen Herausforderungen verbunden – nicht etwa, weil es an Regelungen mangelt, sondern weil es eine Vielzahl an Vorgaben aus unterschiedlichsten Rechtsbereichen gibt. Der Einsatz von KI betrifft nicht nur spezielle Vorschriften wie die KI-VO, sondern ist eingebettet in ein umfassendes Netz horizontaler und sektoraler Regelwerke. In vielen Fällen ist der Einsatz von KI nicht nur zulässig, sondern sogar erforderlich, um regulatorische Vorgaben überhaupt einhalten zu können.

Zurecht erfährt die neue KI-VO, die im Jahr 2024 verabschiedet wurde, große Aufmerksamkeit. Sie stellt zweifellos einen Meilenstein in der Regulierung von KI dar. Ihr risikobasierter Ansatz konzentriert sich jedoch vorrangig auf spezifische Hochrisiko-Anwendungen – etwa im Bereich der biometrischen Identifikation, kritischer Infrastrukturen oder der Bewertung von Personen. Nach Einschätzung der Europäischen Kommission fallen allerdings nur etwa 5 bis 15 Prozent der derzeit am Markt befindlichen KI-Systeme tatsächlich unter den Anwendungsbereich der Verordnung.

Es wäre daher ein Fehlgriff, sich allein auf die KI-VO zu stützen. Weitere Rechtsakte – insbesondere die DS-GVO – behalten ihre volle Geltung. Das gilt insbesondere dann, wenn KI-Systeme personenbezogene Daten verarbeiten oder mit solchen Daten

[2] TÜV- Verband, Verbraucher: innen fordern gesetzliche Regeln für Künstliche Intelligenz,21.11.2022, abrufbar unter: Verbraucher:innen fordern gesetzliche Regeln für Künstliche Intelligenz – TÜV-Verband (zuletzt abgerufen am 23.05.2025).

trainiert wurden. In diesen Fällen greifen KI-VO und DS-GVO parallel, was durch Art. 2 Abs. 7 der KI-VO ausdrücklich bestätigt wird. In der Praxis kann dies zu Spannungsverhältnissen oder Zielkonflikten führen.

Je nach Einsatzkontext können darüber hinaus weitere Rechtsakte einschlägig sein – sei es, weil sie explizit KI-Regelungen enthalten oder weil der Einsatz von KI faktisch erforderlich ist, um gesetzliche Pflichten einzuhalten.

So kann der Einsatz von KI beispielsweise zur Abwehr von Cybergefahren erforderlich sein – etwa zur Erfüllung der Anforderungen aus Art. 32 DS-GVO, Art. 21 der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Richtlinie (EU)2022/2555) (NIS-2-Richtlinie) oder Art. 9 ff. der Verordnung über die digitale operationale Resilienz des Finanzsektors (Verordnung (EU) 2022/2554) (DORA). Konkrete Anwendungsfelder umfassen hier etwa die Erkennung von Bedrohungen (Threat Detection), die Reaktion und Eindämmung (Response and Mitigation), das Schwachstellenmanagement (Vulnerability Management), die durch Künstliche Intelligenz unterstützte Bedrohungssuche (KI-gestützte Threat Hunting) sowie eine effizientere Auswertung für Sicherheitsanalystinnen und -analysten (Streamlined Analyst Experience).

Darüber hinaus relevante gesetzliche Vorschriften:

1. **Produktsicherheit, Produkthaftung und Cybersecurity**

- Produkthaftungsrichtlinie: Erfasst KI als potentiellen Schadensverursacher; haftungsrelevant bei mangelhafter Cybersicherheit oder Fehlfunktionen.
- General Product Safety Regulation (GPSR): Legt Sicherheitsanforderungen auch für KI-gestützte Produkte fest.
- Cybersecurity Act (CSA): Schafft ein EU-weites Zertifizierungssystem, das auch sicherheitsrelevante KI-Anwendungen erfassen kann.

2. **Datenzugang, Interoperabilität und digitale Märkte**

- Data Act: Regelt den fairen Zugang zu Daten, insbesondere aus vernetzten Produkten – KI kann zur Analyse großer Datenmengen oder zur semantischen Interoperabilität beitragen.
- Daten-Governance-Verordnung (DGA): Schafft Rahmenbedingungen für Datenintermediäre – KI kann technische Maßnahmen zur datenschutzfreundlichen Umsetzung unterstützen.
- Digital Services Act (DSA): Reguliert Plattformen, die auch KI-gestützte Empfehlungssysteme oder Moderation betrifft.
- Digital Markets Act (DMA): Regelt Gatekeeper-Plattformen, deren KI-Systeme oft das Marktverhalten beeinflussen.
- eIDAS-Verordnung: Ermöglicht den Einsatz von KI bei der biometrischen Identitätsprüfung oder zur Fälschungserkennung in Vertrauensdiensten.

3. **Sektorale Spezialvorgaben**

- European Health Data Space (EHDS): Fördert den Einsatz von KI in der medizinischen Forschung und Diagnostik. Die Verordnung ist am 26. März 2025 in Kraft getreten, ihre Vorschriften finden jedoch erst schrittweise ab dem 26. März 2027 Anwendung.
- MiCA-Verordnung: Im Kryptobereich kann KI zur Risikobewertung und automatisierten Compliance-Überwachung beitragen.
- Corporate Sustainability Reporting Directive (CSRD): KI kann erforderlich sein, um strukturierte ESG-Berichte gemäß neuen Standards zu erstellen.

4. **Deutsches Recht**

- Bundesdatenschutzgesetz (BDSG): Relevanz bei der Verarbeitung von Beschäftigtendaten durch KI-Systeme – z. B. bei Scoring- oder Auswahlverfahren.
- Telekommunikation-Digitale-Dienste-Datenschutzgesetz (TDDDG): Anwendung bei KI-gestützter Nutzeranalyse in Online-Diensten.

2 Checkliste zum datenschutz-konformen Einsatz von KI

Die Nutzung von KI im Unternehmen bietet Chancen zur Prozessoptimierung und Erschließung neuer Geschäftsmodelle. Sie bringt jedoch auch rechtliche und ethische Herausforderungen mit sich, insbesondere im Datenschutz. Diese Checkliste unterstützt Entscheidungsträger, Projektmanager und technische Fachkräfte bei der Einführung und Nutzung von KI-Technologien. Sie gewährt eine strukturierte Übersicht der wesentlichen Schritte und Maßnahmen zur Einhaltung der DS-GVO und Minimierung von Risiken für die Rechte der betroffenen Personen.

Die Checkliste ist in zwei Bereiche unterteilt:

1. **Training eigener KI-Modelle:**
   Dieser Teil der Checkliste behandelt die Schritte und Maßnahmen, die bei der Entwicklung und dem Training von KI-Modellen notwendig sind. Dazu gehören beispielsweise die Auswahl und Dokumentation des Modells sowie die Klassifizierung und Verarbeitung von Trainingsdaten unter Berücksichtigung datenschutzrechtlicher Anforderungen.
2. **Nutzung von KI-Systemen:**
   Dieser Teil der Checkliste fokussiert sich auf die Nutzung bestehender KI-Systeme und die Einhaltung datenschutzrechtlicher Vorgaben im operativen Einsatz. Hier werden Aspekte wie die Risikobewertung, die Dokumentationspflichten und die Sensibilisierung der Mitarbeiter behandelt.

Hinweis:
Die Checkliste ist nicht abschließend und erhebt keinen Anspruch auf Vollständigkeit. Je nach Anwendungsfall empfiehlt es sich, die Checkliste ggf. um Aspekte außerhalb des Datenschutzrechts sowie spezielle betriebliche Vorgaben zu ergänzen. Bei komplizierten Fragestellungen bietet es sich an, sich einen Überblick über die vorhandenen Äußerungen der Aufsichtsbehörden zu verschaffen. Als Ausgangspunkt eignet sich hierfür der Orientierungshilfen-Navigator des Landesbeauftragten für Datenschutz und Informationsfreiheit.[3]

[3] LfDI Baden-Württemberg, ONKIDA, Orientierungshilfen-Navigator KI & Datenschutz, abrufbar unter: ONKIDA. Orientierungshilfen-Navigator KI & Datenschutz(zuletzt abgerufen am 23.05.2025).

Training eigener KI-Modelle und Systeme

1. Feststellung des Personenbezugs

- ☐ Wurden personenbezogene Daten (direkt oder indirekt identifizierbar) verwendet?
- ☐ Wurden Grenzfälle (z. B. pseudonymisierte Daten, Fahrzeugdaten, IDs) bewertet?
- ☐ Wurde geprüft, ob eine Re-Identifizierung realistisch ist (z. B. bei Verwendung öffentlich verfügbarer Quellen)?

2. Rechtsgrundlage für die Datenverarbeitung (Art.6, 9 DSGVO)

- ☐ Berechtigtes Interesse nach Art. 6 Abs. 1 lit. f geprüft (inkl. Dreistufentest: Interesse – Erforderlichkeit – Abwägung)?
- ☐ Einwilligung (Art. 6 Abs. 1 lit. a / Art. 9 Abs. 2 lit. a) eingeholt – inkl. Widerrufsmöglichkeit?
- ☐ Vertragserfüllung (Art. 6 Abs. 1 lit. b) als Grundlage vertretbar?
- ☐ Zulässigkeit von Zweckänderung und Weiterverarbeitung dokumentiert?
- ☐ Nutzung anonymisierter oder aggregierter Daten erwogen?

3. Besondere Kategorien personenbezogener Daten

- ☐ Liegt ein Ausnahmetatbestand nach Art. 9 DSGVO vor?
- ☐ Zusätzliche Schutzmaßnahmen für sensible Daten implementiert?

4. Datenschutzgrundsätze

- ☐ Zweckbindung klar definiert (z. B. Training für bestimmte Anwendungsfälle)?
- ☐ Datenminimierung, Speicherbegrenzung und Richtigkeit berücksichtigt?
- ☐ Fairness, Transparenz und Rechenschaftspflicht gewährleistet?

5. Technische und organisatorische Maßnahmen (TOM) und »Privacy by Design«

- ☐ Datenschutzfreundliche Technikgestaltung (»Privacy by Design«) umgesetzt?
- ☐ Datenschutzfreundliche Voreinstellungen (»Privacy by Default«) realisiert?

- ☐ Relevante Maßnahmen getroffen:
  - ☐ Berechtigungskonzepte
  - ☐ Löschkonzept
  - ☐ Interne KI- Nutzungsrichtlinie
  - ☐ Incident – Response – Prozesse (Datenschutzvorfälle)
  - ☐ Benennung eines Datenschutzbeauftragten
  - ☐ Verzeichnis der Verarbeitungstätigkeiten geführt?
  - ☐ DSFA durchgeführt (bei hohem Risiko) (die DSFA nach Art. 35 DSGVO ist mit der Grundrechten Folgenabschätzung nach Art.27 KI-VO zu koordinieren)
  - ☐ AV-Verträge und ggf. Standardvertragsklauseln abgeschlossen?
  - ☐ TOMs auch im Sinne der KI-VO anpassen, z. B. bei Risikomanagementprozessen (vgl. Stiftung Datenschutz, Praxisleitfaden zum Anonymisieren personenbezogener Daten)[4]

Nutzung von KI-Systemen und Modellen

1. Personenbezug in der Nutzung erkennen

- ☐ Können durch Nutzung personenbezogene Daten generiert, rekonstruiert oder verarbeitet werden (z. B. durch Prompting oder Output)?
- ☐ Besteht die Gefahr einer »Regurgitation« (Wiedergabe von Trainingsdaten)?

2. Rechtsgrundlage für Nutzung

- ☐ Liegt eine gültige Rechtsgrundlage für die Eingabe und Verwendung personenbezogener Daten im Prompt vor?
- ☐ Wurde die Nutzung des Modells dokumentiert (Transparenz, Zweckbindung)?
- ☐ Wurde die Drittanbieter-KI datenschutzrechtlich bewertet?

3. Betroffenenrechte und Transparenz

- ☐ Wurde die Nutzung KI-gestützter Systeme gegenüber Betroffenen offengelegt?
- ☐ Möglichkeit zur Auskunft oder Löschung sichergestellt?

[4] Stiftung Datenschutz, Praxisleitfaden zum Anonymisieren personenbezogener Daten, Dezember 2022, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Studie_Praxisleitfaden-Anonymisieren-Web_01.pdf (zuletzt abgerufen am 23.05.2025).

- ☐ Profiling und automatisierte Entscheidungen nach Art. 22 DSGVO bewertet?[5]

4. Technische & organisatorische Maßnahmen

- ☐ Verträge mit KI-Anbietern geprüft (z. B. AV-Verträge)?
- ☐ Zugriffskontrollen und Rechtevergabe dokumentiert?
- ☐ Wurde eine DSFA (Art.35 DSGVO) durchgeführt?
- ☐ Wurden die Verarbeitungstätigkeiten in das Verzeichnis aufgenommen und dokumentiert?
- ☐ Logging und Monitoring implementiert?
- ☐ Anonymisierungspfade bei der Nutzung geprüft?
- ☐ Rollenklärung und Verantwortlichkeit
- ☐ Ist die eigene Rolle geklärt (Verantwortlicher, Auftragsverarbeiter, gemeinsam Verantwortlicher)? (vgl. DSK- Orientierungshilfe KI und Datenschutz)[6]
- ☐ Wurde eine Risikoabwägung zur Nutzung externer KI durchgeführt?

5. Implementierung unternehmensinterner Prozesse

- ☐ Einbeziehung der erforderlichen Stakeholder
- ☐ Erstellung und Umsetzung unternehmensinterner Nutzungsvorgaben für KI-Systeme

[5] DSK, Künstliche Intelligenz und Datenschutz, Orientierungshilfe, Version 1.0, 06.05.2024, Rn.33, abrufbar unter: 20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf (zuletzt abgerufen am 23.05.2025).
[6] DSK, Künstliche Intelligenz und Datenschutz, Orientierungshilfe, Version 1.0, 06.05.2024, Rn.33, abrufbar unter: 20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf (zuletzt abgerufen am 23.05.2025).

3 DS-GVO-Anforderungen

Einführung: Personenbezug und Anonymität

Der Anwendungsbereich der DS-GVO erstreckt sich auf personenbezogene Daten (Art. 1 Abs. 1 DS-GVO). Gem. Art. 4 Nr. 1 DS-GVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Nicht umfasst sind anonyme Daten, d. h. Angaben, bei denen der Personenbezug endgültig beseitigt wurde (Erwägungsgrund. 26 S. 5 DS-GVO) (ErwGr.).

Eine Person gilt als identifiziert, wenn ihre Identität unmittelbar aus der Information hervorgeht (z. B. Name). Eine Person ist identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung (z. B. IP-Adresse, Cookie-ID) oder zu besonderen Merkmalen identifiziert werden kann (Art. 4 Nr. 1 DS-GVO). Entscheidend ist, ob eine (Re-)Identifizieung der natürlichen Person möglich ist.

Bei der Beurteilung sind gemäß ErwGr. 26 S. 3 und 4 DS-GVO alle Mittel zu berücksichtigen, die vom Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen vernünftigerweise wahrscheinlich genutzt werden, um die Person direkt oder indirekt zu identifizieren. Hierfür sind alle objektiven Faktoren wie die Kosten und der erforderliche Zeitaufwand, die zum Zeitpunkt der Verarbeitung verfügbare Technologie und deren Weiterentwicklung zu berücksichtigen. Illegale Mittel bleiben nach der Rechtsprechung des EuGH[7] außer Betracht. Die praktische Möglichkeit der Identifizierung ist entscheidend.

Ob es sich bei bestimmten Informationen um personenbezogene Daten im Sinne der DS-GVO handelt, ist nicht immer eindeutig zu beurteilen. Ein anschauliches Beispiel hierfür bietet die Entscheidung des EuGH vom November 2023 in der Rechtssache C-319/22 Gesamtverband Autoteile-Handel e.V. gegen Scania CV AB.[8] In diesem Vorabentscheidungsverfahren, das vom LG Köln angestrengt wurde, ging es um die Frage, ob Fahrzeughersteller verpflichtet sind, Fahrzeug-Identifikationsnummern (FIN) gegenüber unabhängigen Wirtschaftsakteuren offenzulegen. Entscheidend war, ob eine FIN ein personenbezogenes Datum im Sinne der DS-GVO darstellt.

Der EuGH stellte klar, dass eine FIN nicht per se als personenbezogenes Datum einzustufen ist (Rn. 46). Sie kann jedoch dann personenbezogen sein, wenn der betreffende Akteur vernünftigerweise über Mittel verfügen kann, mit denen sich die FIN einer identifizierten oder identifizierbaren natürlichen Person zuordnen lässt. In einem solchen Fall handele es sich sowohl für die unabhängigen Wirtschaftsakteure als auch – mittelbar – für den Fahrzeughersteller um personenbezogene Daten. Ob im konkreten Fall eine solche Zuordnung möglich ist, wurde vom EuGH offengelassen und dem vorlegenden Gericht zur weiteren Prüfung überlassen (Rn. 49).

[7] EuGH, Urt vom 19.10.2026 ; Rs.C- 582/14.
[8] EuGH, Urt vom 09.11.2023, Rs. C-319/22.

Diese Überlegungen zur potenziellen Identifizierbarkeit gelten auch für moderne Technologien, insbesondere für KI. Die Verarbeitung personenbezogener Daten durch KI-Systeme, sei es beim Training oder im Betrieb, fällt unter die DS-GVO. Eine besondere Herausforderung stellt die Beurteilung dar, ob KI-Modelle selbst (insbesondere Large Language Models, LLMs) oder die von ihnen generierten Ausgaben (Outputs) personenbezogene Daten darstellen.

Der Europäische Datenschutzausschuss (EDSA) hat in seiner Stellungnahme 28/2024[9] klargestellt, dass KI-Modelle, die mit personenbezogenen Daten trainiert wurden, nicht pauschal als anonym angesehen werden können. Ein Modell gilt nur dann als anonym, wenn das Risiko, dass personenbezogene Daten aus den Trainingsdaten

(1) direkt aus dem Modell extrahiert werden können (z. B. durch »Membership Inference Attacks« oder »Model Inversion Attacks«) oder

(2) aus den Abfragen (Outputs) des Modells gewonnen werden können (»Regurgitation«),

unter Berücksichtigung aller vernünftigerweise wahrscheinlichen Mittel vernachlässigbar gering (»insignificant«) ist.

Die technische Funktionsweise von LLMs (z. B. Tokenisierung, Speicherung von Parametern/Vektoren statt Klartext) allein schließt danach einen Personenbezug nicht aus, wenn die genannten Risiken bestehen. Die Beweislast, dass ein Modell anonym ist, liegt nach Ansicht des EDSA beim Verantwortlichen. Dieser muss dies gegenüber der Aufsichtsbehörde umfassend dokumentieren und nachweisen können (EDSA Opinion 28/2024, Rn. 34, 56 ff.). Gelingt dieser Nachweis nicht, unterliegt das Modell bzw. dessen Training/Nutzung weiterhin der DS-GVO.

Texte, Bilder oder andere Daten, die von einem KI-System generiert werden, können ebenfalls personenbezogene Daten sein. Dies ist unproblematisch der Fall, wenn der Output sich auf eine identifizierte Person bezieht (z. B. KI generiert einen Text über Max Mustermann). Personenbezug kann aber auch vorliegen, wenn der Output die (Re-)Identifizierung einer Person ermöglicht, z. B. durch die Reproduktion von Trainingsdaten oder durch die Generierung neuer, aber auf eine Person beziehbarer Informationen (z. B. Wahrscheinlichkeitsaussagen, »Halluzinationen«, die einer realen Person zugeordnet werden können). Auch hier gilt der Maßstab der vernünftigerweise wahrscheinlichen Identifizierbarkeit.

Eine wirksame Anonymisierung von Daten vor dem KI-Training oder des KI-Modells selbst setzt voraus, dass der Personenbezug nach den oben genannten Kriterien (vernachlässigbares Extraktions-/Inferenzrisiko) dauerhaft beseitigt wird. Die Anforderungen sind hoch und der Nachweis ist komplex. Techniken wie Differential Privacy oder Federated Learning können das Risiko reduzieren, führen aber nicht automatisch zur Anonymität.

Die Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) reduziert zwar Risiken, beseitigt den Personenbezug aber nicht. Daten bleiben pseudonym, solange die Zuordnung zu einer Person mit Zusatzinformationen möglich ist. Die Frage, ob Daten für einen Empfänger,

[9] EDSA, Stellungnahme des EDSA zu KI-Modellen: DSGVO – Prinzipien unterstützen verantwortungsvolle KI, 28/2024 vom 18. 12. 2024, abrufbar unter: Stellungnahme des EDSA zu KI-Modellen: DSGVO-Prinzipien unterstützen verantwortungsvolle KI | European Data Protection Board (zuletzt abgerufen am: 23.05.2025).

der nicht über das Zusatzwissen zur Re-Identifizierung verfügt, als anonym gelten können (relative Anonymität), ist für Datentransfers relevant und wurde vom EuGH (SRB/EDSB T-557/20)[10] tendenziell bejaht. Gegen dieses Urteil legte der EDSB am 05.06.2023 Rechtsmittel beim EuGH ein. Das Verfahren trägt das Aktenzeichen C-413/23 P. Der EDSB macht geltend, dass das EuGH die Begriffe »personenbezogene Daten« und »pseudonymisierte Daten« gemäß der Verordnung (EU) 2018/1725 fehlerhaft ausgelegt habe.[11] Für die Bewertung des KI-Modells selbst legt der EDSA jedoch einen strengeren Maßstab an (Fokus auf allgemeines Extraktionsrisiko, dass jemand personenbezogenen Daten extrahieren könnte, unabhängig vom konkreten Empfänger).[12]

Die ursprüngliche Herausforderung des sog. »Prompt Engineering«, bei den Nutzenden durch geschickte Eingaben versuchen, die KI zur Preisgabe (ggf. personenbezogener) Informationen zu bewegen oder zu manipulieren, ist ein Beispiel für das Risiko der Datenextraktion aus Abfragen. Dieses Risiko ist bei der Beurteilung der Anonymität eines Modells nach EDSA explizit zu berücksichtigen. Ebenso ist das »Hintergrund-wissen« der KI, also die in den Parametern repräsentierten statistischen Zusammen-hänge, die Quelle für das Inferenzrisiko.

Artikel 5 DS-GVO: Einhaltung der Datenschutzgrundsätze

Rechtmäßigkeit, Art. 5 Abs.1lit. a Alt. 1 DS-GVO

Die Rechtmäßigkeit der Verarbeitungen im Rahmen der Entwicklung, des Trainings und der Verwendung eines KI-Systems und Modells umfasst sowohl das »Ob« (Rechtsgrundlage) als auch das »Wie« der Verarbeitung (Einhaltung sonstiger datenschutzrechtlicher Vorgaben zu Modalitäten einer Verarbeitung personen-bezogener Daten). Auf der Grundlage von Art. 8 (II) der Charta der Grundrechte der Europäischen Union setzen insbesondere Art. 5 Abs.1lit. a und Art. 6, 9 DS-GVO diesen Grundsatz um. Zusätzlich sind auch etwaige nationale Vorgaben bei der Beurteilung der Rechtmäßigkeit heranzuziehen, soweit sie sich im Rechtsetzungsspielraum der DS-GVO halten. Grundsätzlich gilt – sowohl aus rechtlichen als auch aus praktischen Gesichtspunkten – entsprechend Art. 25 DS-GVO –, alle daten-schutzrechtlichen Anforderungen an KI-Modelle und Systeme direkt vom Beginn der Entwicklung und im Rahmen des Designs mitzuberücksichtigen. Dies erleichtert auch die spätere Umsetzung der Anforderungen.

Hinweis: Werden im Rahmen einer Pilotierung von KI-Modellen oder Systemen personenbezogene Daten verarbeitet, müssen bereits zum Zeitpunkt des Beginns der

[10] EuGH. Urt. Vom 26.04.2023, Rs. T-557/20.
[11] EuGH, Rs. C 413/23 P, Rechtsmittel des EDSB gegen EuG, Urt. v. 26.4.2023 – T 557/20, eingelegt am 5. Juli 2023 GH, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?text=&docid=276483&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (zuletzt abgerufen am 23.05.2025).
[12] EDSA, Stellungnahme des EDSA zu KI-Modellen: DSGVO – Prinzipien unterstützen verantwortungsvolle KI, 28/2024 vom 18. 12. 2024, abrufbar unter: Stellungnahme des EDSA zu KI-Modellen: DSGVO-Prinzipien unterstützen verantwortungsvolle KI | European Data Protection Board (zuletzt abgerufen am: 23.05.2025).

Pilotierung die DS-GVO-Anforderungen, insbesondere in Bezug auf die Rechtmäßigkeit, erfüllt sein. Insoweit gibt es für Pilotphasen keine »Schonfrist«.

Im Hinblick auf die verschiedenen Verarbeitungsphasen eines KI-Systems oder Modells (Erhebung, Training, Bereitstellung, Nutzung, Weiterentwicklung) können unterschiedliche Rechtsgrundlagen einschlägig sein. Eine Datenverarbeitung ist nur zulässig, wenn eine Erlaubnistatbestand gegeben ist (sog. Verbot mit Erlaubnisvorbehalt.

Hinweis: Der EDSA hat in seiner Stellungnahme zur Verarbeitung personenbezogener Daten in KI-Systemen klargestellt, dass für verschiedene Verarbeitungsphasen separate Rechtsgrundlagen erforderlich sein können. Der EDSA hebt hervor, dass die Wahl der Rechtsgrundlage von der spezifischen Phase der Datenverarbeitung und den jeweiligen Umständen abhängt. Demnach ist wichtig, dass jede Phase der Datenverarbeitung sorgfältig geprüft wird, um sicherzustellen, dass die gewählte Rechtsgrundlage den Anforderungen der DS-GVO entspricht

Die Einhaltung der Anforderungen gemäß der Position des EDSA kann in der Praxis herausfordernd sein. Dies bedeutet, dass sich Verantwortliche als Erstes einen Überblick über die unterschiedlichen Verarbeitungsvorgänge in den einzelnen Phasen und ggf. einschlägigen bzw. divergierenden Rechtsgrundlagen verschaffen müssen. Ein Ergebnis kann zum Beispiel sein, dass für die Phase der Erhebung eine Einwilligung eingeholt werden soll und ein Widerrufsmanagement etabliert werden muss, während eine nachfolgende Verarbeitung auf berechtigte Interessen gestützt werden soll und ein Widerspruchsmanagement umgesetzt werden müsste. Noch anspruchsvoller wäre die Situation, gesetzt den Fall, dass besondere Kategorien personenbezogener Daten hinzukommen und Anforderungen nach Art. 9 DS-GVO beachtet werden müssten.

Praxistipp: Um diesen Herausforderungen in der Praxis zu begegnen, ist aus unternehmerischer Sicht empfehlenswert, nach Möglichkeit eine einzige Rechtsgrundlage zu finden, welche sämtliche Verarbeitungsvorgänge über alle Phasen hinweg abdeckt. Dies hat u. a. Vorteile beim Monitoring und der Dokumentation zum Zweck der Erfüllung von Nachweispflichten gemäß Art. 5 Abs.2 DS-GVO sowie im Rahmen der Bearbeitung von Betroffenenrechten. Es ist daher wichtig, die einzelnen Verarbeitungstätigkeiten und verfolgten Zwecke je Phase gedanklich zu antizipieren, um ein strukturiertes und effizientes Vorgehen zu erreichen. Einen hilfreichen Überblick zum AI-Lifecycle bietet der International Standard ISO/IEC 5338.

Grundsätzlich kommen hierfür alle Rechtsgrundlagen der KI-VO, DS-GVO (insb. Art. 6 und 9 DS-GVO), aber auch nationale Gesetze in Betracht, da die DS-GVO für KI-Modelle oder Systeme keine speziellen Rechtsgrundlagen vorsieht.

Schon im Rahmen der Erhebung/Veredlung von Trainingsdaten und der entsprechenden Nutzung dieser Daten für Zwecke des Trainings von KI-Systemen und Modellen wird regelmäßig die Frage nach der Zweckbindung bzw. Zweckänderung zu stellen sein. Oftmals wird der Wunsch bestehen, vorhandene Datenbestände zum Training nutzbar zu machen. Für Zwecke der Innovationsförderung wird Art. 54 der KI-VO in Zukunft unter engen Voraussetzungen eine Weiterverarbeitung für ursprünglich zu anderen Zwecken erhobene Daten innerhalb von Sandboxes zulassen (Art. 6 Abs.4 DS-GVO i. V. m. Art. 54 KI-VO).

Regelmäßig wird man Art. 6 Abs.1 lit. b DS-GVO (Erfüllung eines Vertrages oder Durchführung vertraglicher Verpflichtungen) als Rechtsgrundlage heranziehen können, wenn nach objektiver Betrachtung die Verarbeitung des KI-Modells oder

Systems wesentlicher Bestandteil der Hauptleistungspflichten eines Vertrags mit einem Datensubjekt bzw. einer betroffenen Person sind, so z. B. bei Nutzung von generativen KI-Modellen und Systemen zur Erzeugung von Texten oder Bildern. Schwieriger ist die Beurteilung, wenn in Zukunft KI-Modelle oder Systeme unterstützend bei der Erbringung vertraglicher Leistungen in unterschiedlichem Intensitäts- oder Wirkungsgrad eingesetzt werden, z. B. beim Einsatz von zum Teil personalisierten Chatbots im Rahmen des Kundenservices für eine Dienstleistung/ein Produkt. Hier ist eine Beurteilung im Einzelfall erforderlich, inwieweit die Verarbeitung noch objektiv erforderlich ist.

Soweit die Einwilligung als Rechtsgrundlage herangezogen werden soll, wird sich ein Schwerpunkt in der Bewertung der ausreichenden Verständlichkeit (»in informierter Weise«, s. a. Art. 4 Abs.11 DS-GVO und entsprechender Formulierung) ergeben. Im Zusammenspiel mit den Informationspflichten (Art. 12 ff. DS-GVO) sollte auf eine konsistente Darstellung geachtet werden. Artikel 12 Abs.1 DS-GVO fordert zusätzlich eine »präzise« Information, welches der Transparenz in gewisser Weise entgegenstehen kann, soweit sehr komplexe technische Verarbeitungsvorgänge betroffen sind.

Problematisch sind auch Fälle des Widerrufs der Einwilligung, soweit im Modell noch personenbezogene Daten verarbeitet werden bzw. aus diesem extrahiert werden können. Die Sicherstellung dieser Anforderung muss unter dem Gesichtspunkt des Privacy-by-Design von Anfang an bedacht werden.

In diesem Zusammenhang sei letztlich auf die sorgfältige Prüfung der Freiwilligkeit (ErwGr 42 S. 5 DS-GVO) der Abgabe von Einwilligungserklärungen gerade im Arbeitsverhältnis (§ 26 Abs. 2 BDSG; ErwGr 43 DS-GVO), aber nicht nur, hingewiesen (siehe auch unten bei »Rechtsgrundlage bei der Nutzung von personenbezogenen Daten zu Trainingszwecken«). Mitarbeitende müssen eine echte freie Wahl haben. Durch eine Verweigerung dürfen dem Mitarbeitenden keine beruflichen Nachteile entstehen, so dürfte er z. B. eine gleichwertige Alternative zu der KI-Verwendung erhalten. Bei Bewerbenden wird man in der Regel immer von einem Nachteil ausgehen können, da bei einer Verweigerung der Einwilligung mit einer Nichtberücksichtigung der Bewerbung zu rechnen ist. Ist die Einwilligung des Mitarbeitenden nicht der alleinige Erlaubnistatbestand für die Datenverarbeitung, muss der Arbeitgeber darauf hinweisen, dass er die Daten auch auf andere Grundlage als die Einwilligung des Arbeitnehmers verarbeiten könnte, und sich dies auch ausdrücklich vorbehalten. Anderenfalls kann sich der Arbeitgeber nicht auf (weitere) gesetzlichen Rechtsgrundlagen berufen, falls die Einwilligung unwirksam sein sollte.

Im Arbeitsverhältnis ist als Rechtsgrundgrundlage für eine Datenverarbeitung auch an eine (Gesamt)Betriebsvereinbarung zu denken (§ 26 Abs. 4 BDSG). Aber diese hat sich nach der aktuellen Rechtsprechung des EuGH auch an die Anforderungen der DS-GVO zu halten, so insbesondere auch aus Art. 5, Art. 6 Abs. 1 und Art. 9 DS-GVO. Das Schutzniveau der DS-GVO darf nicht durch eine (Gesamt)Betriebsvereinbarung unterschritten werden (siehe dazu auch unten »Rechtsgrundlage bei der Nutzung von personenbezogenen Daten zu Trainingszwecken«). Bestehende (Gesamt)Betriebsvereinbarungen sind darauf hin zu überprüfen und ggf. anzupassen.

Treu und Glauben, Art. 5 Abs.1 lit. a Alt. 2 DS-GVO

Der Grundsatz, wonach die Verarbeitung »nach Treu und Glauben« zu erfolgen hat, findet eher weniger praktische Relevanz. Bekannt ist er als unbestimmter Rechtsbegriff des Generaltatbestands nach § 242 BGB. Die deutsche Gesetzgebung definiert den Begriff als redliches, aufrichtiges Sozialverhalten. Als Norm für den Privatrechtsverkehr ist diese Definition jedoch nicht einfach auf die DS-GVO zu übertragen. Es liegt daher näher, auf die englische Fassung mit der Bezeichnung »Fairness« abzustellen, auch wenn diese ähnlich schwammig ist.

Unter unfairen Datenverarbeitungen werden beispielsweise verborgene, unerwartete oder unverhältnismäßige Verarbeitungen subsumiert. Dabei liegen Überschneidungen mit den anderen Grundsätzen auf der Hand und erklären abermals die untergeordnete Rolle dieses Grundsatzes.

In Bezug auf KI-Systeme und Modelle, bei denen wir vorwiegend von Lernsystemen sprechen, wären zu berücksichtigende Aspekte im Rahmen der unverhältnismäßigen Verarbeitungen die Nutzung von Big Data als Grundlage für das Machine Learning und eben die Frage nach der Verhältnismäßigkeit und Erforderlichkeit dieses enormen Datenumfangs.

Hinsichtlich des gewählten Modells, der Lizenz, der Einbettung und der Konfiguration stellt sich die Frage, mit welchen Daten/aus welchen Datenquellen das Modell gelernt hat. Weiterhin stellt sich die Frage, ob auch anhand eigener Dateninputs gelernt wird, inwieweit das Recht auf Vergessenwerden beeinträchtigt wird, und ob die eventuelle Verwendung und Speicherung unerwartet und unfair sein kann.

Selbst im Falle einer eingeholten Einwilligung zur Datenverarbeitung wäre die Umsetzung des »Rechts auf Widerruf« nur schwer durchsetzbar und damit nicht im Rahmen der geforderten »Fairness«. Eine noch »unfairere« Situation wäre wohl, wenn die Nutzung einer KI für den Betroffenen erst gar nicht ersichtlich wäre (»verborgen«).

Bei der Frage der Erkennbarkeit und Transparenz der KI-Nutzung ist auch die Schutzwürdigkeit von Geschäftsgeheimnissen zu berücksichtigen. Eine vollständige Offenlegung der Nutzung von KI-Systemen kann mit berechtigten Geheimhaltungsinteressen – etwa hinsichtlich der konkreten Funktionsweise, der verwendeten Trainingsdaten oder der Modellarchitektur – kollidieren. Diese Interessen sind im Rahmen einer fairen Abwägung ebenfalls angemessen zu berücksichtigen.

Darüber hinaus ist ein weiterer Aspekt zu berücksichtigen: Sofern die Trainingsquellen und herangezogenen Daten unbekannt sind, bleibt auch verborgen, ob der Ergebnis-Output aufgrund einseitiger, stereotypischer Daten erfolgt, und damit nicht repräsentativ wäre. Es entstünde eine »algorithmische Diskriminierung«.

Vor dem Einsatz eines KI-Systems oder Modells sollte daher innerhalb einer Risikoprüfung eruiert werden, ob eine Diskriminierung vorliegen könnte und somit Rechte und Freiheiten von betroffenen Personen gefährdet wären. Im Unternehmenskontext wäre ein zu berücksichtigender Punkt die Chancengleichheit am Arbeitsplatz.

Transparenz, Art. 5 Abs.1lit. a Alt. 3 DS-GVO

Sobald ein Unternehmen personenbezogene Daten verarbeitet, ist es verpflichtet, dies transparent zu tun, indem es den Betroffenen verständlich und in einer einfachen Sprache informiert. Diese Pflicht bezieht sich sowohl auf eine Erhebung der Daten direkt bei der oder dem Betroffenen als auch bei einer Erhebung durch Dritte (Art. 13, 14 DS-GVO). Unternehmen haben daher beim Einsatz von KI die erste Hürde bereits dadurch zu überwinden, dass sie technisch anspruchsvolle KI-Lösungen in eine einfache und verständliche Sprache übersetzen müssen. Von der Datenverarbeitung betroffene Personen müssen über diese Datenverarbeitung dann hinreichend informiert werden.

Um dem Grundsatz einer hinreichenden Transparenz nachzukommen, ist Verantwortlichen zu empfehlen, ihre Datenschutzerklärungen und -richtlinien sowie Datenschutzhinweise im Arbeitsverhältnis dahingehend zu aktualisieren, dass der Einsatz sowie der Zweck verwendeter KI beschrieben wird. Auch die Logik hinter KI-gestützten automatisierten Entscheidungen sowie mögliche Risiken sollten verständlich dargelegt werden.

Detailliertere Ausführungen zur Transparenz finden sich unter dem Punkt »Transparenz und Informationspflichten«.

Neben den Anforderungen aus der Datenschutzgrundverordnung werden auch mit Inkrafttreten der KI-VO weitere Transparenzpflichten zu erfüllen sein. Der Umfang wird abhängig von der Risikoklassifizierung variieren, als Mindestanforderung jedoch eine KI-Kennzeichnung sowie Transparenzerklärung beinhalten.

Zweckbindung, Art. 5 Abs.1lit.b DS-GVO

Fraglich ist weiterhin, ob bereits einmal zu einem bestimmten Zweck erhobene Daten durch eine weitere Verarbeitung in einem KI-System oder Modell und einem neu entstandenen Kontext eine nicht erlaubte Zweckänderung darstellen. Es bedarf jeweils einer Einzelfallprüfung, ob diese Weiterverarbeitung für

- im öffentlichen Interesse liegende Archivzwecke,
- wissenschaftliche oder
- historische Forschungszwecke oder
- statistische Zwecke

vorgenommen wurde, damit sie nicht als unvereinbar mit den ursprünglichen Zwecken und dem Kompatibilitätstest gilt.

Im Einklang mit dieser strengen Auslegung ist jedoch die Nutzung von Daten, die bereits keinen Personenzug mehr aufweisen, also anonymisiert wurden oder solche, die aus öffentlich zugänglichen Quellen eingesetzt werden.

Bei der Nutzung derartiger Daten würden die weiteren Tatbestandsmerkmale des Art. 5 DS-GVO, nämlich die Speicherbegrenzung sowie Integrität und Vertraulichkeit der personenbezogenen Daten, nicht mehr tangiert.

Datenminimierung, Art. 5 Abs.1lit.c DS-GVO

Der Grundsatz der Datenminimierung sieht vor, dass Unternehmen personenbezogene Daten nur für bestimmte, erforderliche Zwecke verarbeiten und speichern. Es handelt sich um eine Ausprägung des Verhältnismäßigkeitsgrundsatzes, der eine Verhältnismäßigkeitsprüfung erfordert. Die Verarbeitung von personenbezogenen Daten ist daher grundsätzlich auf das notwendige Maß zu beschränken.

Auch hier besteht die Schwierigkeit in der Abwägung, da zur Durchführung des Trainings der KI i. d. R. große Datenmengen (»Big Data«) herangezogen werden. Sollten Unternehmen (bspw. zum Finetuning) ihr KI-Modell oder System trainieren, ist vorab eine Verhältnismäßigkeitsprüfung durchzuführen und die »Zweck-Mittel-Relation« zwischen dem Sammeln der Daten und Effizienz des Trainings zu bestimmen. Insbesondere das Mittel der (irreversiblen) Anonymisierung der Trainingssätze stellt eine Möglichkeit dar, datenschutzkonform vorzugehen.

Richtigkeit, Art. 5 Abs.1lit.d DS-GVO

Aufgrund der möglichen Konsequenzen von Falschinformationen für Betroffene verlangt die DS-GVO grundsätzlich, dass nur sachlich richtige personenbezogene Daten verarbeitet werden. Unrichtige personenbezogene Daten sind unverzüglich zu löschen oder zu berichtigen.

Es kommt jedoch regelmäßig vor, dass ein Large Language Model Halluzinationen erzeugt. Es handelt sich hierbei um unrichtige Informationen, die zunächst plausibel erscheinen können. Halluzinationen kollidieren mit dem Grundsatz der Richtigkeit. Betroffenen Personen steht zudem nach Art. 16 DS-GVO ein Recht auf Berichtigung zu.

Ergebnisse der KI sind daher kritisch zu hinterfragen und zu verifizieren, auch im Falle von Plausibilität.

Rechenschaftspflicht, Art. 5 Abs.2 DS-GVO

Die Rechenschaftspflicht stellt ein zentrales Prinzip der DS-GVO dar. Sie besagt, dass Verantwortliche nicht nur sicherstellen müssen, dass sie die Vorschriften der DS-GVO einhalten, sondern auch nachweisen können müssen, dass sie dies tun. Verantwortliche müssen angemessene technische und organisatorische Maßnahmen implementieren, um die Sicherheit und den Schutz personenbezogener Daten zu gewährleisten.

Noch immer konnten Unklarheiten bzgl. des Umfangs und der Form der Rechenschaft nicht in Gänze ausgeräumt werden, sodass einem restriktiven Verständnis, dass diesen Anforderungen nur mittels eines Datenschutzmanagementsystems begegnet werden könne, die Kritik am »One size fits all«-Ansatz und der Angemessenheit für kleinere Unternehmen entgegengesetzt wird.

Unabhängig davon, ob interne Mechanismen und Kontrollsysteme (Plan-Do-Check-Act, PDCA) eingerichtet, oder Prozesse mit Personenbezug aktenmäßig dokumentiert werden, ist zu gewährleisten, dass den Aufsichtsbehörden Nachweise vorgelegt werden können.

Zu den Maßnahmen zählen **insbesondere**

- das Führen eines Verzeichnisses von Verarbeitungstätigkeiten
- interne Datenschutzrichtlinien
- die Dokumentation von Datenschutzverletzungen
- Prozessdokumentationen
- der Abschluss von Auftragsverarbeitungsverträgen (ggf. Standardvertragsklauseln)
- die Durchführung von Datenschutzfolgenabschätzungen
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design und Privacy by Default)
- die Benennung eines Datenschutzbeauftragten

Diese Nachweise beziehen sich auch auf die Gewährleistung der datenschutzrechtlichen Grundsätze beim Einsatz von KI und deren Verschriftlichung.

Bereits das Global Privacy Assembly 2020.[13] forderte im Falle einer Entwicklung oder Nutzung von KI u. a. zu folgenden Rechenschaftsmaßnahmen auf:

- Bewertung und Offenlegung der potenziellen Auswirkungen auf die Menschenrechte (einschließlich der Rechte auf den Schutz der Daten und der Privatsphäre) vor Nutzung der KI
- Führen von Verzeichnissen über die Folgenabschätzung, die Konzeption, die Entwicklung, die Prüfung und die Verwendung von KI
- Die Gewährleistung der Transparenz und Offenheit durch Offenlegung der Nutzung von KI, der verwendeten Daten und der Logik der KI

Um der Rechenschaftspflicht nachzukommen, ist insbesondere eine Dokumentation obiger Maßnahmen in einem angemessenen Rahmen umzusetzen.

Rechtsgrundlage bei der Nutzung von personenbezogenen Daten zu Trainingszwecken

Das Vorliegen einer Rechtsgrundlage ist ein wesentlicher Schritt für eine rechtskonforme Verarbeitung personenbezogener Daten für KI-Training. Als Rechtsgrundlage kommen grundsätzlich die Verarbeitung zur Wahrung berechtigter Interessen für Unternehmen im nicht öffentlichen Bereich in Betracht (Art. 6 Abs. 1 lit. f DS-GVO), die Einwilligung (Art.6 Abs.1 lit. a DSGVO) sowie die Verarbeitung im Rahmen der Vertragserfüllung (Art. 6 Abs.1 lit. b DS-GVO). Die KI-VO schafft – abgesehen von den eng auszulegenden Tatbeständen des Art. 10 Abs. 5 KI-VO (Bias-Korrektur bei

[13] LDA Brandenburg, Entschließung zur Rechenschaftspflicht bei der Entwicklung und Nutzung der künstlichen Intelligenz, abrufbar unter: 42. GA: Rechenschaftspflicht bei Entwicklung und Nutzung der KI | Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (zuletzt abgerufen am 23.05.2025). LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0 vom 17.10.2024, abrufbar unter: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (zuletzt abgerufen am 23.05.2025).

Hochrisiko-KI) und Art. 59 KI-VO (Weiterverarbeitung in regulatorischen Sandkästen) – keine neuen, eigenständigen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Training. Sie verweist in Art. 2 Abs. 7 KI-VO explizit auf die Anwendbarkeit der DS-GVO.

Berechtigtes Interesse

Im Bereich der KI ist das berechtigte Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO eine für die Praxis besonders relevante Rechtsgrundlage. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist – sofern nicht die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person überwiegen.

Laut dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)[14] kommt dieser Norm im Kontext von KI eine besondere Bedeutung zu. Die Formulierung des berechtigten Interesses ist vergleichsweise offen und bietet dadurch eine gewisse Flexibilität, insbesondere bei innovativen datengetriebenen Anwendungen. Im Unterschied zu anderen Rechtsgrundlagen bedarf Art. 6 Abs. 1 lit. f DSGVO keiner weiteren nationalen oder europäischen Ausgestaltung.

Diese Offenheit kann jedoch auch zu Rechtsunsicherheit führen. Gerade bei komplexen KI-gestützten Verarbeitungsprozessen hängt die rechtliche Bewertung stark vom konkreten Kontext und den getroffenen Schutzmaßnahmen ab.

In seiner Stellungnahme 28/2024 vom 18. Dezember 2024 befasst sich der EDSA ausführlich mit der Anwendung von Art. 6 Abs. 1 lit. f DSGVO im Kontext von KI-Modellen.[15] Darin stellt der Ausschuss klar, dass Unternehmen sicherstellen müssen, dass die Verarbeitung rechtmäßig, transparent und auf das erforderliche Maß begrenzt erfolgt. Der EDSA empfiehlt einen dreistufigen Test, um zu beurteilen, ob das berechtigte Interesse als Rechtsgrundlage geeignet ist. Hierzu gehören folgende Schritte:

(1) Verfolgung eines berechtigten Interesses: Es muss ein berechtigtes Interesse des Verantwortlichen oder eines Dritten vorliegen. Dies kann wirtschaftlicher, rechtlicher oder sonstiger Natur sein.

(2) Erforderlichkeit der Verarbeitung: Die Verarbeitung personenbezogener Daten muss erforderlich sein, um das berechtigte Interesse zu verfolgen. Es darf keine weniger invasive Methode zur Erreichung des Ziels geben.

[14] LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0 vom 17.10.2024, abrufbar unter: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (zuletzt abgerufen am 23.05.2025).
[15] EDSA, Stellungnahme des EDSA zu KI-Modellen: DSGVO – Prinzipien unterstützen verantwortungsvolle KI , 28/2024 vom 18. 12. 2024, abrufbar unter: Stellungnahme des EDSA zu KI-Modellen: DSGVO-Prinzipien unterstützen verantwortungsvolle KI | European Data Protection Board (zuletzt abgerufen am: 23.05.2025).

KI-Training mit Daten aus öffentlichen Nutzerprofilen

Das OLG Köln hat mit Beschluss vom 23.05.2025 (Az. 15 UKl 2/25) den Antrag der Verbraucherzentrale NRW auf Erlass einer einstweiligen Verfügung gegen das KI-Training mit öffentlich geposteten Daten auf Facebook und Instagram zurückgewiesen.[16] Hintergrund: Meta Platforms Ireland Limited hatte im April 2025 angekündigt, ab dem 27.05.2025 personenbezogene Daten aus öffentlich zugänglichen Nutzerprofilen für das Training von KI-Systemen zu verwenden. Die Verbraucherzentrale NRW leitete daraufhin am 12.05.2025 ein Eilverfahren ein.

Entscheidung: Das Gericht stellte im Rahmen der summarischen Prüfung fest, dass kein Verstoß gegen die DSGVO vorliege. Die beabsichtigte Datenverarbeitung könne auch ohne Einwilligung auf das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Meta verfolge mit dem Training seiner KI-Modelle ein legitimes Interesse, das nicht auf milderem Weg erreichbar sei.

Das OLG betont, dass ausschließlich öffentlich zugängliche Daten verarbeitet werden sollen, die auch über Suchmaschinen auffindbar sind. Zwar können auch große Datenmengen betroffen sein, darunter Inhalte von Dritten, Minderjährigen oder potenziell sensible Daten im Sinne des Art. 9 DSGVO – diese überwiegen im Rahmen der Interessenabwägung jedoch nicht.

Meta hatte die Verarbeitung bereits im Jahr 2024 angekündigt. Nutzer wurden über verschiedene Kanäle (z. B. Apps) informiert und haben die Möglichkeit, der Verarbeitung durch Privatsphäre-Einstellungen oder Widerspruch zu widersprechen. Zudem würden laut Meta keine eindeutigen Identifikatoren wie Name, E-Mail-Adresse oder Postanschrift verarbeitet.

Anwendungsbeispiel aus der Automobilindustrie

KI kommt in der Automobilindustrie etwa zum Einsatz, wenn es um das Training von hoch- und vollautomatisierten (§§ 1a ff. StVG) sowie autonomen Fahrfunktionen (§§ 1d ff. StVG) geht. Für das Training sind vielfältige Daten aus Erprobungsfahrten erforderlich, mittels derer etwa die sog. Objekterkennung und Objektklassifizierung bei sicherheitsrelevanten Verkehrssituationen verbessert wird. Dafür ist es notwendig, möglichst viele Verkehrssituationen und -szenarien sowie verschiedene Objekte und Straßenverkehrsteilnehmenden sowie Passanten zu erfassen. Die Quantität und Qualität der verwendeten Trainingsdaten bestimmt insoweit die Wahrscheinlichkeit, dass eine KI-basierte Sicherheitsfunktion eine Verkehrssituation richtig analysiert und führt damit zu einer Steigerung der Verkehrssicherheit. Nach dem aktuellen Stand der Technik bedarf es hierfür noch immer Daten aus »echten« Verkehrssituationen – Aufnahmen von Testgeländen oder die Nutzung von synthetischen Daten liefern kein gleichwertiges Ergebnis. Dasselbe gilt für die Nutzung von Datensätzen, die mittels Software zunächst anonymisiert oder pseudonymisiert worden sind, bevor sie zum Anlernen der Sicherheitsfunktionen genutzt werden. Denn das Pseudonymisieren/Anonymisieren der Daten als eine Art »Verfälschung« der Aufnahmen mit dem Ziel, Gesichter oder Kennzeichen beispielsweise durch Unschärfe oder Schwärzen

[16] OLG Köln, Besch. v. 23.05.2025, Az. 15 UKl. 2/25, abrufbar unter: OLG Köln, Urteil vom 23.05.2025 – 15 UKl 2/25 – openJur zuletzt abgerufen am 30.06.2025.

unkenntlich zu machen, erhöht die Wahrscheinlichkeit, dass reale Situationen im Straßenverkehr von den Fahrassistenzsystemen nicht eindeutig erkannt werden. In dem Zusammenhang ist zu berücksichtigen, dass die Erkennung von Personen nur dann alle Personengruppen gleichwertig abdeckt, wenn Teile der Trainingsdaten Aufnahmen sämtlicher Personengruppen und damit auch von Kindern, Personen mit Mobilitätseinschränkungen usw. beinhalten. Um einen gleichwertigen Schutz aller Personengruppen zu gewährleisten, bedarf es daher insbesondere auch Aufnahmen von besonders schutzwürdigen Personengruppen, aber auch Verkehrsräumen, wie bspw. Krankhauseinfahrten und Spielstraßen, in denen sich besondere Gefahrensituationen ereignen können. Somit stehen sich im Rahmen der Erforderlichkeitsabwägung – neben weiteren Aspekten – insbesondere der Grundsatz der Datenminimierung und das allgemeine, öffentliche Interesse an der Erhöhung der Verkehrssicherheit gegenüber.[17]

Der Vollständigkeit halber sei erwähnt, dass das Vorliegen der Erforderlichkeit jeweils für die unterschiedlichen Test- und Entwicklungsphasen zu prüfen ist. Das heißt, können in einigen Entwicklungsphasen technische und organisatorische Maßnahmen ergriffen werden, um die Anzahl der Betroffenen oder auch den Grad der Betroffenheit zu verringern, sind diese Maßnahmen zu ergreifen. Solche Maßnahmen können etwa sein: Durchführung der Erprobungsfahrten zu verkehrsberuhigten Zeiten; Wahl von Kamerawinkeln, bei denen möglichst wenig Gesichter aufgenommen werden; Vermeidung von Quasi-Überwachungssituationen, indem möglichst auf Mehrfachaufnahmen desselben Orts, zur selben Tageszeit verzichtet wird, und bei atypischen Standzeiten, d. h. nicht lediglich ampelbedingter Halt, die Aufnahmesensorik ausgeschaltet wird.

(3) Abwägung der Interessen: Die Interessen, Grundrechte und Freiheiten der betroffenen Personen müssen gegen das berechtigte Interesse abgewogen werden. Die Verarbeitung darf die Rechte der betroffenen Personen nicht übermäßig beeinträchtigen.

Besondere Abwägungskriterien im KI-Kontext sind:

- Art der Daten: Sensibilität, Kategorie (z. B. Gesundheits- oder Bewegungsdaten)
- Umfang und Granularität der Trainingsdaten
- Auswirkungen auf die betroffenen Personen (z. B. bei automatisierten Entscheidungen)
- Art des ML-Verfahrens: insbesondere hinsichtlich Transparenz, Nachvollziehbarkeit und Datenverarbeitungstiefe
- Anzahl der beteiligten Verarbeiter oder Dritten
- Dauer der Datenverarbeitung
- Technische und organisatorische Maßnahmen (TOMs): z. B. Pseudonymisierung, Zugriffsbeschränkungen, Auditverfahren

[17] DSK, Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten, Beschluss der DSK vom 27.09.2023, abrufbar unter: DSK_Positionspapier_audiovisuelle_Umgebungserfassung.pdf (zuletzt abgerufen am 32.05.2025).

Diese Schritte helfen sicherzustellen, dass die Verarbeitung personenbezogener Daten auf einer soliden rechtlichen Grundlage erfolgt und die Rechte der betroffenen Personen gewahrt bleiben.

Einwilligung

Die Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO kann eine Rechtsgrundlage sein, insbesondere wenn ein direktes Verhältnis zur betroffenen Person besteht und die hohen Anforderungen der DS-GVO (Art. 4 Nr. 11, Art. 7 DS-GVO – Informiertheit, Freiwilligkeit, Widerruflichkeit) erfüllt werden können. Bei komplexen KI-Trainingsprozessen stellt insbesondere die Anforderung der Informiertheit und die technische Umsetzbarkeit des Widerrufsrechts (potenzielle Notwendigkeit des Neutrainierens bei Widerruf) eine erhebliche Hürde dar. Bei der Sammlung von Trainingsdaten aus dem Internet (Webscraping) oder von Dritten ist die Einholung einer wirksamen Einwilligung in der Regel praktisch unmöglich. Auch eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO für die Verarbeitung besonderer Kategorien ist unter diesen Umständen kaum realisierbar.

Vertragserfüllung

Eine Datenverarbeitung kann nur dann auf die Erfüllung eines Vertrages gemäß Art. 6 Abs.1 lit. b DS-GVO gestützt werden, wenn ein konkretes vertragliches oder vorvertragliches Verhältnis zwischen der betroffenen Person sowie der oder dem Verantwortlichen besteht. Dabei ist zu beachten, dass die Verarbeitung ein objektiv erforderlicher Vertragsbestandteil sein muss. In Hinblick auf die Verarbeitung von personenbezogenen Daten zu KI-Trainingszwecken scheidet ein vertragliches Verhältnis in aller Regel aus, da die Verarbeitung objektiv nicht zur Vertragserfüllung erforderlich ist und eine entsprechende Regelung einer AGB-Kontrolle nicht standhalten würde. Anders sieht es nur dann aus, wenn das KI-Training Vertragsbestandteil ist (z. B. Erstellung eines KI-Sprachgenerators, der mit der Stimme der betroffenen Person trainiert wird)[18]. Zu beachten ist, dass keine vertragliche Vereinbarung geschlossen werden kann, die die Verarbeitung personenbezogener Daten von Dritten zu KI-Trainingszwecken legitimiert.

Rechtliche Verpflichtung; Wahrnehmung einer Aufgabe von öffentlichem Interesse; Betriebsvereinbarung

Die Anforderungen, welche für Art. 6 Abs.1 lit. b DS-GVO »Erfüllung eines Vertrages« gelten, sind ebenso gültig für Datenverarbeitungen, welche auf die Art. 6 Abs.1 lit. c - e.

DS-GVO gestützt werden. Jedoch gibt es bisher keine rechtliche Verpflichtung für nicht öffentliche Stellen zum Einsatz von KI zu Trainingszwecken.

Der Einsatz von KI kann grundsätzlich auch in einer Betriebsvereinbarung geregelt werden. Allerdings darf das Schutzniveau der DS-GVO in diesem Fall nicht

[18] LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0 vom 17.10.2024, S.13,abrufbar unter: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (zuletzt abgerufen am 23.05.2025).

unterschritten werden. Zudem muss das anwendbare Tarifrecht sowie Betriebsverfassungsrecht gewahrt werden. Aufgrund der eben genannten Hürden, der wegen des Vorlagebeschlusses des EuGH bestehenden Rechtsunsicherheiten[19] sowie dem Aspekt, dass der Einsatz von KI zu Trainingszwecken mit hoher Wahrscheinlichkeit die Interessen der betroffenen Personen nicht überwiegt, eignet sich eine Betriebsvereinbarung als Legitimationsgrundlage nicht.

Die aktuell öffentlich zugängliche Fassung der KI-Verordnung sieht die Möglichkeit der Weiterverarbeitung zuvor rechtmäßig erhobener personenbezogener Daten zur Entwicklung bestimmter KI-Systeme und Modelle im öffentlichen Interesse im KI-Reallabor grundsätzlich vor. Aufgrund des engen Anwendungsbereichs und der sehr hohen Anforderungen wird diese Regelung jedoch nur in Ausnahmefällen zur Anwendung kommen können.

Zweckänderung

Eine Zweckänderung ist nach Art. 6 Abs.4 DS-GVO nur dann zulässig, wenn sie mit dem ursprünglichen Zweck vereinbar ist und eine rechtliche Grundlage hat. Verantwortliche müssen die Konformität ihrer eigenen Verarbeitungsoperationen vollständig analysieren. Insbesondere muss der Verantwortliche die Transparenzanforderungen erfüllen. Es wird daher nur schwer möglich sein, vorhandene, für einen ursprünglichen Zweck vorgesehen Daten unter dem Gesichtspunkt der Zweckänderung für Trainingszwecke zu verwenden.

Ein denkbarer use case in der Praxis ist eine Weiterverarbeitung personenbezogener Daten zum Zweck der Verbesserung eines Produktes, für dessen Nutzung die Daten ursprünglich erhoben wurden.

Soweit eine Zweckänderung nach Art. 6 Abs.4 DS-GVO im Einzelfall als unzulässig eingeschätzt wird, kommt alternativ eine Neuerhebung von Daten auf Basis einer der vorgenannten Rechtsgrundlagen in Betracht. Dies ist in der Praxis allerdings angesichts der damit einhergehenden Aufwände (Zeit, Kapazitäten und Kosten) allenfalls ultima ratio und rechtlich nicht unumstritten.

Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor

Eine zusätzliche Rechtsgrundlage mit Blick auf eine Weiterverarbeitung von personenbezogenen Daten ist in Art. 59 KI-VO geregelt. Als eine Maßnahme zur Innovationsförderung richtet sich die Rechtsgrundlage an Behörden, juristische sowie natürliche Personen, welche ein KI-System entwickeln. Dies unter engen und kumulativ zu erfüllenden Voraussetzungen, wie insbesondere, dass eine solche Entwicklung unter der zuständigen Aufsicht im öffentlichen KI-Reallabor geschieht und der Wahrung eines erheblichen öffentlichen Interesses in einem oder mehreren abschließend benannten Bereichen, wie z. B. öffentliche Sicherheit und öffentliche Gesundheit,

[19] AG Vorlagebeschluss an EuGH vom 22.09.2022 – 8 AZR 209/21.

Umweltschutz, nachhaltiger Energie, Sicherheit von Verkehrssystemen usw. dient. In Deutschland wird derzeit intensiv an der Umsetzung von KI-Reallaboren gearbeitet, um innovative KI-Technologien zu testen und zu entwickeln. Im November 2024 hat die Bundesregierung einen entsprechenden Gesetzesentwurf für ein sog. ReallaboreG vorgelegt. Die weitere Entwicklung und Akzeptanz in der Praxis bleibt abzuwarten.

Verwendung anonymisierter oder aggregierter Daten

Als mögliche Lösung dieser vielfältigen Probleme kommt die Verwendung anonymisierter oder aggregierter Daten in Betracht (hinsichtlich der Begriffe »relative und absolute Anonymität« siehe Kapitel: Einführung Begriffe »relative und absolute Anonymität« auf Seite 17). Da es sich bei diesen Daten nicht mehr um personenbezogene Daten handelt, ist der Anwendungsbereich der DS-GVO nicht eröffnet.

Für das Training könnten sich daher aggregierte Daten eignen, da bei der Aggregation von Daten Fallgruppen im aktiven Datensatz zu einzelnen Fällen kombiniert, die dann als separate aggregierte Datei abgespeichert werden. In diesem Fall kann der Personenbezug entfallen, wenn sich die aggregierten Daten nicht auf eine bestimmte natürliche Person, sondern auf eine Personengruppe beziehen. Dies bedarf einer Prüfung des jeweiligen Einzelfalls.

Sowohl die Anonymisierung von Daten als auch die Erstellung aggregierter Datensätze stellt nach vorherrschender Meinung eine Verarbeitung personenbezogener Daten dar, sodass eine Rechtsgrundlage hierfür notwendig ist. In Betracht kommt das berechtigte Interesse – wobei in der Feststellung dessen die Abwägung eine entscheidende Rolle spielt.

Problematisch ist dabei jedoch, dass die betroffenen Personen ein Widerspruchsrecht haben. Wenn die Daten bereits anonymisiert sind, besteht aufgrund der Anonymisierung keine Möglichkeit mehr, diesem Recht effektiv Rechnung zu tragen.

Dieser scheinbare Widerspruch kann jedoch damit aufgelöst werden, da die DS-GVO nach der Anonymisierung der Daten keine Anwendung mehr findet.

Im Allgemeinen ist auch der Begriff der Anonymität nicht einheitlich und klar gesetzlich definiert. Der Begriff war bereits Streitpunkt vieler gerichtlicher Entscheidungen, sowohl auf nationaler als auch auf internationaler Ebene. Es lohnt sich daher, in die Absicherung der Anonymisierung von Daten einen hohen Aufwand zu investieren. Dabei können die Ausführungen in der Checkliste im letzten Kapitel dieses Papiers helfen.

Artikel 9 DS-GVO: Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten (nachfolgend: sensible Daten) umfasst nach Art. 9 Abs.1 DS-GVO, Daten zu der rassischen und ethnischen Herkunft, der politischen Meinung, religiösen oder weltanschaulichen Überzeugungen, der Gewerkschaftszugehörigkeit, genetischen und biometrischen Daten, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Den sensiblen Daten gemeinsam ist, dass die

Kenntnis derer von anderen Personen und insoweit deren Verarbeitung für die betroffenen Personen erhöhte Risiken für ihre Grundrechte und Freiheiten mit sich bringen kann. Vor dem Hintergrund sehen die gesetzlichen Regelungen strengere Anforderungen an die Verarbeitung sensibler Daten vor (u. a. Vorhandensein einer speziellen Rechtsgrundlage nach Art. 9 Abs.2 DS-GVO/Spezialgesetz sowie erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen), vgl. auch ErwGr 51 ff. DS-GVO. Gleichzeitig kann die Verarbeitung sensibler Daten für die betroffenen Personen von großem Vorteil und in ihrem Interesse sein, z. B.:

- die KI-gestützte Befundung in der bildgebenden Diagnostik;
- Applikationen zur Unterstützung von Patientinnen und Patienten (z. B. in Form von Chatbots).

Mit Blick auf die jüngste Rechtsprechung (BGH-Urteile des Bundesgerichtshofs vom 27. März 2025, Az. I ZR 222/19 und I ZR 223/19 in Umsetzung des Urteils des Europäischen Gerichtshofs vom 4.10.2024 in der Rechtssache C-21/23) ist hierbei zu beachten, dass genau zu prüfen ist, ob sensible Daten vorliegen. So können Angaben, die auf den ersten Blick nicht sensibel erscheinen, aufgrund gedanklicher Ableitung/ Rückschlüssen in den Schutzbereich des Art. 9 DSGVO fallen, z. B. wenn auf Basis des Kauf- und Surfverhaltens die Wahrscheinlichkeit einer Schwangerschaft oder einer bestimmten Erkrankung nahe liegt. In solchen Konstellationen ist daher bereits frühzeitig zu überlegen, ob die strengeren Anforderungen an die Verarbeitung sensibler Daten eingehalten werden müssen. Es empfiehlt sich, diese Überlegungen und schließlich das Ergebnis zu dokumentieren.

Welche DS-GVO-Rechtsgrundlagen kommen für die Verarbeitung sensibler Daten im KI-Kontext in Betracht?

Die Einholung einer Einwilligung nach Art. 9 Abs.1lit. a DS-GVO geht mit einer Vielzahl an praktischen Herausforderungen einher (vgl. insoweit die Ausführungen im vorherigen Abschnitt zu den Rechtsgrundlagen). Darüber hinaus eröffnet Art. 9 Abs.2 DS-GVO u. a. Verarbeitungsmöglichkeiten in den Bereichen der Sozialfürsorge (einschließlich der Erfüllung arbeitsrechtlicher Pflichten), des Gesundheitswesens, aber auch der Forschung – wobei der Art. 9 Abs2 DS-GVO jedoch u. a. bei der Regelung zur Verarbeitung von sensiblen Daten zu Forschungszwecken nach Buchstabe j) (in Verbindung mit Art. 89 DS-GVO) das Vorliegen einer EU- oder nationalen Regelung vorsieht.[20] Auftrieb im Bereich der Gesundheitsforschung sollen insoweit auch § 6 Gesundheitsdatennutzungsgesetz (GDNG) und auf europäischer Ebene der Europäische Raum für Gesundheitsdaten (EDHS) geben, wobei bis zur Geltung der EU-Vorschriften über die sog. Sekundärnutzung der Patientendaten noch Jahre vergehen werden.[21] Eine taugliche Rechtsgrundlage für die Verarbeitung von sensiblen Daten mittels KI scheint Art. 9 Abs.2 lit. e DS-GVO zu sein, wonach die Verarbeitung zulässig ist, wenn sich diese auf sensible Daten bezieht, die die betroffene Person offensichtlich

[20] nationale Regelungen können sein: § 27 BDSG; Regelungen in den Landeskrankenhausgesetzen, z. B. § 25 Berliner Landeskrankenhausgesetz, § 27 Bayerisches Krankenhausgesetz, § 37 Landeskrankenhausgesetz Rheinland-Pfalz oder § 6 Gesundheitsdatenschutzgesetz Nordrhein-Westfalen; Regelungen in den Landesdatenschutzgesetzen, z. B. § 22 Landesdatenschutzgesetz Rheinland-Pfalz, § 24 Hessisches Datenschutz- und Informationsfreiheitsgesetz oder § 13 Niedersächsische Datenschutzgesetz; Regelungen zur Forschung mit Sozialdaten der Krankenkassen, z. B. § 75 SGB X zum Zugang von Forschenden zu Sozialdaten, § 67c Abs. 5 SGB X bei internen Forschungsvorhaben von Leistungsträgern.

[21] EU-Kommission, EHDS, abrufbar unter: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_de (zuletzt abgerufen am: 23.05.2025).

öffentlich gemacht hat. Die Regelung ist jedoch (wie die übrigen Ausnahmeregelungen des Art. 9 DS-GVO) eng auszulegen. Das heißt nicht alle sensiblen Daten, die im Internet veröffentlicht sind, dürfen frei genutzt werden. Vielmehr ist zu prüfen, ob die betroffene Person erkennbar keinen Wert auf den Schutz ihrer sensiblen Daten mehr legt. Da die subjektive Wahrnehmung, wann etwas »privat« ist und wann nicht, sehr variiert, lässt sich selbst bei Daten, die im Internet verfügbar sind, selten auf den 1. Blick sagen, ob eine Verarbeitung auf Art. 9 Abs.2 lit. e DS-GVO gestützt werden kann. Für die Beurteilung spielen bspw. das Vorhandensein von Einstellmöglichkeiten, die Default-Einstellungen der Webseite/Web-Anwendung, die tatsächlichen Privatsphäre-Einstellungen der betroffenen Personen oder auch die zur Verfügung gestellten (Datenschutz-)Informationen eine Rolle (vgl. EuGH-Urteil vom 4. Juli 2023, C-252/21). Der EuGH stellte in seinem Urteil vom 4. Juli 2023 darüber hinaus u.a. noch die folgenden Aspekte heraus:

- Art. 9 Abs.2 lit. e DS-GVO gilt nicht für Daten, die von anderen Personen veröffentlicht worden sind als denjenigen, die sie betreffen (vgl. Rn. 75);
- die betroffenen Personen muss die Absicht gehabt haben, die fraglichen personenbezogenen Daten ausdrücklich und durch eine eindeutige bestätigende Handlung der breiten Öffentlichkeit zugänglich zu machen (vgl. Rn. 77).

Vor dem Hintergrund muss vor der Nutzung von im Internet veröffentlichten sensiblen Daten geprüft werden, ob die Ausnahmevorschrift des Art. 9 Abs.2 lit. e DS-GVO Raum für die Nutzung der Daten im KI-Kontext schafft und die Erkenntnisse/Gründe dokumentiert werden, um im Fall der Fälle das Prüfergebnis begründen zu können.

Folgen für den Einsatz von KI-Modellen bei DS-GVO-widrigem KI-Training

Bei der Prüfung der Rechtsgrundlage ist regelmäßig die Frage zu berücksichtigen, ob das im Unternehmen genutzte KI-Modell rechtmäßig trainiert worden ist. Aber welche Maßnahmen sind zu ergreifen, wenn personenbezogene Daten rechtswidrig für das KI-Training verwendet wurden, etwa weil es an einer geeigneten Rechtsgrundlage fehlte? Welche Folgen hat eine unzulässige Verarbeitung im Training für die spätere Nutzung des Modells? Sind derartige Modelle überhaupt noch rechtskonform einsetzbar?

Antworten auf diese Fragen gibt die »Stellungnahme 28/2024« des EDSA.[22] Diese Stellungnahme bietet eine erste europäische Orientierung zur datenschutzrechtlichen Beurteilung von KI-Modellen, insbesondere zur Folgeproblematik unrechtmäßiger Trainingsdaten.

[22] EDSA, Stellungnahme des EDSA zu KI-Modellen: DSGVO – Prinzipien unterstützen verantwortungsvolle KI, 28/2024 vom 18. 12. 2024, abrufbar unter: Stellungnahme des EDSA zu KI-Modellen: DSGVO-Prinzipien unterstützen verantwortungsvolle KI | European Data Protection Board, (zuletzt abgerufen am: 23.05.2025).

Die rechtliche Einschätzung des Europäischen Datenschutzausschusses

Der EDSA entwickelt ein auf Szenarien basierendes Prüfmodell, das als Orientierungshilfe für die Praxis dient. Die Kernaussage lautet, dass die Rechtswidrigkeit des Trainings die spätere Nutzung des Modells unzulässig machen kann, wobei dies nicht zwingend der Fall ist.

Im Einzelnen unterscheidet der EDSA zwischen folgenden Konstellationen:

Szenario 1: Weiterverwendung des KI-Modells durch denselben Verantwortlichen

Im ersten Szenario wird ein KI-Modell, das unter Verstoß gegen die DS-GVO trainiert wurde, vom ursprünglichen Verantwortlichen selbst weiterverwendet. Wenn personenbezogene Daten im KI-Modell verbleiben und der Verantwortliche das Modell später selbst einsetzt, muss geprüft werden, ob Entwicklungs- und Nutzungsphase denselben oder unterschiedlichen Zwecken dienen. Werden in beiden Phasen die Daten für denselben Zweck verarbeitet, handelt es sich datenschutzrechtlich um einen einheitlichen Verarbeitungsvorgang. In diesem Fall wirkt sich ein etwaiger Datenschutzverstoß aus der Entwicklungsphase auch auf die Nutzungsphase aus – mit der Folge, dass die gesamte Verarbeitung rechtswidrig ist.

Anders kann es sich verhalten, wenn die Zwecke der Verarbeitung in der Entwicklungs- und Nutzungsphase voneinander abweichen. Dann ist im Einzelfall zu prüfen, ob und in welchem Umfang sich die ursprüngliche Rechtswidrigkeit auf die spätere Nutzung auswirkt. Insbesondere wenn sich der Verantwortliche bei der Nutzung auf das »berechtigte Interesse« (Art. 6 Abs.1 lit. f DS-GVO) stützt, muss die Interessenabwägung auch die frühere Rechtsverletzung einbeziehen – etwa im Hinblick auf die berechtigten Erwartungen der betroffenen Personen. Es handelt sich also um eine fallbezogene Bewertung, bei der sowohl der Kontext als auch die Risiken für die Betroffenen zu berücksichtigen sind.

Szenario 2: Ein vom KI-Entwickler verschiedenes Unternehmen verwendet das Modell für eigene Zwecke

Wird ein KI-Modell von einem anderen Unternehmen übernommen und für eigene Zwecke eingesetzt, trägt der neue Verantwortliche die datenschutzrechtliche Verantwortung für die Nutzung des Modells. Im Rahmen seiner Rechenschaftspflicht muss er nachweisen können, dass er sich in angemessener Weise mit der Rechtmäßigkeit der ursprünglichen Datenverarbeitung im Training auseinandergesetzt hat. Dies gilt insbesondere dann, wenn bereits Hinweise vorliegen – etwa durch behördliche oder gerichtliche Entscheidungen –, dass das Modell unter Verstoß gegen Datenschutzvorgaben entwickelt wurde. In solchen Fällen kann davon ausgegangen werden, dass der neue Verantwortliche Kenntnis haben musste.

Der EDSA geht in seiner Stellungnahme davon aus, dass dem nutzenden Unternehmen mindestens eine Recherchepflicht obliegt: Es darf sich nicht blind auf die Angaben des Anbieters verlassen. Umfang und Tiefe dieser Prüfung hängen dabei vom Risiko ab, das

mit der Nutzung des Modells verbunden ist – insbesondere dann, wenn potenziell sensible oder risikobehaftete Daten im Modell enthalten sein könnten.

Szenario 3: Das Modell verarbeitet keine personenbezogenen Daten mehr

Wurde ein ursprünglich mit personenbezogenen Daten trainiertes KI-Modell nachträglich so verändert, dass keine Rückschlüsse auf Einzelpersonen mehr möglich sind, gilt es als anonymisiert – und fällt damit nicht mehr in den Anwendungsbereich der DS-GVO. In einem solchen Fall ist die ursprüngliche Rechtswidrigkeit der Datenverarbeitung grundsätzlich nicht mehr relevant, da die Verarbeitung personenbezogener Daten im rechtlichen Sinne nicht mehr fortbesteht. Voraussetzung ist allerdings, dass die Anonymisierung wirksam und irreversibel erfolgt ist. Der Verantwortliche, der das Modell einsetzt, muss dies nicht nur sicherstellen, sondern auch angemessen dokumentieren.

Wird das anonymisierte Modell jedoch in der Nutzungsphase mit neuen personenbezogenen Daten kombiniert – etwa durch Benutzereingaben, Auswertungen oder Rückschlüsse auf Nutzerverhalten –, unterliegt diese neue Verarbeitung selbstverständlich weiterhin den Anforderungen der DS-GVO. In solchen Fällen handelt es sich um eine eigenständige Datenverarbeitung, für die eine geeignete Rechtsgrundlage erforderlich ist. Zudem müssen Betroffenenrechte gewahrt und die Betroffenen ggf. informiert werden.

Zentrale Aussagen des EDSA

- Der EDSA stellt klar, dass die Nutzung eines Modells, das nicht datenschutzkonform trainiert wurde, nicht automatisch verboten ist. Eine Einzelfallprüfung ist erforderlich.
- Unternehmen, die ein vortrainiertes KI-Modell von Dritten übernehmen, sind datenschutzrechtlich verantwortlich. Sie müssen sicherstellen, dass das Modell rechtmäßig trainiert wurde, sich aktiv informieren (»due diligence«) und ggf. Maßnahmen zur Schadensbegrenzung treffen.
- In der Konsequenz bedeutet dies, dass die Behauptung des KI-Modell-Anbieters, das KI-Modell sei rechtmäßig, nicht ausreicht. Wer ein Modell nutzt, muss selbst in der Lage sein, die Rechtmäßigkeit nach bestem Wissen und Gewissen nachzuvollziehen und zu dokumentieren.

Zustimmung seitens deutscher Aufsichtsbehörden

Nach der Veröffentlichung der Stellungnahme 28/2024 wurde deutlich, dass die Datenschutzaufsichtsbehörden in Deutschland die EDSA-Linie grundsätzlich stützen – sie mahnen jedoch auch Konkretisierungen und Unterstützung bei der Umsetzung an.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) begrüßte die Stellungnahme als wichtigen Schritt für mehr Rechtssicherheit im Bereich

KI.[23] Auch die Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und Baden-Württemberg bestätigten die EDSA-Position.[24] Mithin ist empfehlenswert, sich an der Stellungnahme des EDSA zu orientieren, bis weitere konkretisierende Aussagen durch die Aufsichtsbehörden oder im Rahmen von Rechtsprechung getroffen werden.

Transparenz und Informationspflichten

Wie bereits im Kapitel »Einhaltung der Datenschutzgrundsätze des Art. 5 Abs.1DS-GVO erläutert, müssen bei der personenbezogenen Datenverarbeitung gewisse Transparenzgrundsätze eingehalten werden. Eine Analyse der Informationen vom LfDI Rheinland-Pfalz hat gezeigt, dass erheblicher Bedarf für Nachfragen besteht, um bewerten zu können, ob die Regelungen der DS-GVO bei der Datenverarbeitung durch ChatGPT eingehalten werden. Die Forderung nach mehr Transparenz für die Nutzerinnen und Nutzer ist dabei eine wesentliche Komponente. Bei der Entwicklung und dem Einsatz von KI sollte darauf stets besonderes Augenmerk gelegt werden. Einerseits ist Transparenz wichtig, um Akzeptanz und Vertrauen in Anwendungen zu schaffen. Des Weiteren sind gesetzliche Vorgaben zur Transparenz einzuhalten. Neben Transparenzanforderungen, die sich u. a. aus der KI-Verordnung ergeben werden, bleiben die Anforderungen aus der DS-GVO anwendbar. Zu nennen sind insbesondere:

- Das Grundprinzip der Transparenz aus Art. 5 Abs.1 lit. a DS-GVO
- Die Anforderungen aus Kapitel III Abschnitte 1 und 2 (Art. 12-14) DS-GVO
- Sofern Einwilligungen eingeholt werden, die Sicherstellung einer informierten Einwilligung (Art. 6 Abs.1 lit. a, Art. 7 DS-GVO)

Art. 5 Abs.1lit. a DS-GVO macht eine generelle Vorgabe, die Verarbeitung personenbezogener Daten transparent zu gestalten (wofür der Verantwortliche nach Art. 5 Abs.2rechenschaftspflichtig ist). Als umfassendes Prinzip ausgestaltet, lässt die Bestimmung aber offen, wie das im Einzelnen zu erreichen ist. Auch Art. 12 DS-GVO fordert zunächst nur, dass angemessene Maßnahmen zu ergreifen sind, um Informationen in einer transparenten Weise bereitzustellen, verweist aber bereits auf Art. 13 und 14 DS-GVO.

Diese beiden Artikel beinhalten detaillierte Anforderungskataloge, wobei Art. 13 DS-GVO anzuwenden ist, wenn Informationen beim Betroffenen erhoben werden;

Art. 14 DS-GVO findet demgegenüber Anwendung, wenn die Informationen nicht beim Betroffenen, sondern vielmehr ohne seine Mitwirkung bei Dritten erhoben werden.

Die Anforderungen lassen sich wie folgt zusammenfassen (im Einzelfall sollte der Wortlaut der Vorschriften herangezogen werden):

[23] BfDI, BfDI begrüßt EDSA Leitlinien zum berechtigten Interesse, Pressemitteilung 15/2024 vom 09.10.2024, abrufbar unter: BfDI - Pressemitteilungen - BfDI begrüßt EDSA-Leitlinien zum berechtigten Interesse (zuletzt abgerufen am 23.05.2025).
[24] Vgl. gemeinsame Presseerklärung der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und Baden-Württemberg, abrufbar unter:https://www.datenschutz.rlp.de/service/aktuelles/detail/edsa-gibt-orientierungspunkte-fuer-ki#:~:text=Gestaltung,Befugnisse%20der%20Datenschutzbeh%C3%B6rden%20in%20Deutschland (zuletzt abgerufen am 23.05.2025).

- Informationen zum Verantwortlichen und zum Datenschutzbeauftragten
- Zwecke der Verarbeitung und Rechtsgrundlage(n), ggf. auch eine Darlegung der verfolgten legitimen Interessen und der Verarbeitung für weitere Zwecke
- Empfänger von Daten und Drittlandberührungen
- Dauer der Verarbeitung
- Rechte und Beschwerdemöglichkeiten des Betroffenen
- Notwendigkeit einer Bereitstellung der Daten (gesetzlich oder vorvertraglich, beziehungsweise vertraglich)
- Vorliegen einer automatisierten Entscheidung, ggf. Profiling

Art. 14 DS-GVO hat naturgemäß die weitere Anforderung, die betroffene Person über die Herkunft der Daten zu informieren, um ihr so eine Herkunftskontrolle zu ermöglichen.

Im Rahmen von KI sind zwei Aspekte von besonderer Bedeutung: die Frage, wie die Transparenz konkret hergestellt wird und der Punkt zu automatisierten Einzelentscheidungen und Profiling.

a. Es wird oben deutlich, dass eine Reihe von Einzelangaben zu machen sind. Je nach der Art der Anwendung (z. B. Einbindung in umfassendere Systeme, begrenzter Bildschirminhalt, sprach- oder gestengesteuerte Systeme, Verarbeitung im Hintergrund) stellen sich die gleichen Herausforderungen wie bei vielen klassischen KI-freien Anwendungen. Die Komplexität steigt jedoch, wenn zur Tatsache des KI-Einsatzes und zu relevanten Umständen ebenfalls umfassende Angaben zu machen sind. Dieser Aspekt wird sich durch die KI-spezifischen Anforderungen der EU KI-Verordnung weiter verschärfen. Hier kämen im Einzelfall – nicht immer mit der Garantie völliger Rechtssicherheit – die Verwendung von Links, QR-Codes, Symbolen und Piktogrammen oder auch die Bereithaltung klassischer Papierdokumente in Betracht. Hier kommt es ggf. zu besonderen Herausforderungen, wenn Informationen nur auf Umwegen bereitgestellt werden – z. B. wenn in einem Laden oder an öffentlichen Plätzen lediglich Links bzw. QR-Codes publiziert werden, über die weitere Informationen abrufbar sind, während nicht vorausgesetzt werden kann, dass alle Betroffenen diese Informationen zumutbar zeitgleich abrufen können.

b. Wortgleich ist nach Art. 13 und 14 DS-GVO über »das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DS-GVO« zu informieren und es sind darüber hinaus »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.

    a. Art. 22 Abs.1 DS-GVO bezieht sich dabei auf das Recht des Betroffenen, nicht einer ausschließlich automatisierten Entscheidung mit rechtlicher Wirkung oder vergleichbaren Auswirkungen unterworfen zu werden.

    b. Art. 22 Abs. 4) DS-GVO bestimmt enge Grenzen für die Verwendung besondere Arten personenbezogener Daten, wenn in Abweichung von Abs. 1 eine automatisierte Entscheidung ausnahmsweise nach Abs. 2 zulässig ist.

Aufgrund der denkbaren Eingriffstiefe wird häufig intensiverer Kontakt mit einem Betroffenen (z. B. als Kunde, Bewerber) bestehen, sodass diese Informationen außerhalb der eigentlichen KI-Anwendung gegeben werden können. Beabsichtigt eine Versicherung etwa, kleinere Kraftfahrschäden mit geringer Schadenshöhe durch

KI-Einsatz zu automatisieren, sind entsprechende Angaben erforderlich. Das bringt dann ggf. die Gefahr mit sich, dass durch Angaben zur Logik das System oder Modell unsachgemäß beeinflusst und ausgenutzt werden könnte.

Oft wird auch eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1,3 lit. a DS-GVO erforderlich sein. Diese wird im Folgenden auf Seite 50 detailliert erläutert.

Schließlich ist es auch empfehlenswert, signifikante Entscheidungen nicht ausschließlich auf eine automatisierte Entscheidung zu stützen (»human in the loop«, d. h. menschliche Entscheidungsfindung, die ggf. durch KI vorbereitet und unterstützt wird – dieser Schritt sollte aber nicht auf eine rein formelle Prüfung, gleichsam ein Abnicken des KI-Entscheidungsvorschlages, reduziert werden).

Weitere Betroffenenrechte (Art. 12,15 ff. DS-GVO) Artikel 12 ff. DS-GVO: Umsetzung von Betroffenenrechten

Die Umsetzung datenschutzrechtlicher Betroffenenrechte nach Art. 12-21 DSGVO wie insbesondere Ansprüche auf Löschung oder Korrektur personenbezogener Daten befindet sich in einem Spannungsfeld zwischen technischen Limitationen und rechtlichen Anforderungen.

Die Verarbeitung personenbezogener Daten durch KI-Systeme, insbesondere durch Large Language Models (LLMs), führt datenschutzrechtlich zu erheblichen Herausforderungen. Während die DSGVO die Erfüllung der Betroffenenrechte wie Auskunft, Löschung und Berichtigung vorschreibt, erschweren die technischen Besonderheiten von KI-Systemen deren praktische Umsetzung erheblich. Diese Analyse untersucht die spezifischen Herausforderungen und möglichen Lösungsansätze in drei zentralen Szenarien: personenbezogene Daten in den Trainingsdaten, im LLM selbst und bei der Nutzung von KI-Systemen.

1. Szenario: Personenbezogene Daten in Trainingsdaten

Die Umsetzbarkeit und Erfüllung der Betroffenenrechte unterscheidet sich grundlegend je nach Rolle im KI-Ökosystem.

Trainingsdaten werden in der Regel von spezialisierten Datenanbietern oder dem Entwickler/Anbieter des LLM bereitgestellt und aufbereitet. Der KI-System Betreiber, der das Modell einsetzt, hat üblicherweise keine detaillierten Kenntnisse darüber, welche konkreten personenbezogenen Daten in den Trainingsdaten enthalten waren. Vom KI-Anbieter erhält er typischerweise nur generelle Informationen zur Art und Zusammensetzung der Trainingsdaten, ohne Detailinformationen zu konkreten Datenpunkten oder betroffenen Personen.

Die Dokumentation der Trainingsdaten ist oft mangelhaft und bietet keine vollständige Transparenz über enthaltene personenbezogene Informationen. Standardisierte Verfahren zur Identifikation solcher Daten in großen Textsammlungen fehlen häufig. Die Nachverfolgbarkeit der Herkunft einzelner Datenpunkte (Data Lineage) gestaltet sich äußerst schwierig und zuletzt mangelt es meist an einer strukturierten Klassifizierung und Kennzeichnung von Inhalten mit personenbezogenen Daten.

Allerdings ist keine Information notwendig (Art. 14 Abs.5 DS-GVO), wenn sie mit einem unverhältnismäßigen Aufwand verbunden wäre, beispielsweise wegen der großen Zahl der Personen und eventueller Schwierigkeiten bei der Ermittlung

Betroffenenanfragen kann der Betreiber daher faktisch nicht substanziell beantworten, sondern kann nur eine »Auskunft des Nichtwissens« erteilen und kann/sollte die Betroffenenanfragen an die ursprünglichen Datenanbieter oder Modellentwickler weiterleiten.

Verantwortliche können also gut begründen, dass sie in diesen Fällen die Informationspflicht gemäß Art. 14 Abs.5 DS-GVO nicht erfüllen, da dies mit einem unverhältnismäßigen Aufwand verbunden wäre. Gleiches dürfte wohl gelten, wenn eine »Verwässerung der individuellen Betroffenheit« aufgrund einer massenhaften Verarbeitung personenbezogener Daten beim Training/Finetuning von KI-Modellen und Systemen eintritt, sodass die nach DS-GVO erforderliche Betroffenheit unterschritten wird (im Lichte des EuG-Urteils vom 26.4.2023 (Az: T-557/20).

Hat der KI-Betreiber die Trainingsdaten aber selbst erstellt oder direkt von eingekauft, kann und muss er Auskunft darüber geben, ob konkrete Daten einer betroffenen Person in den Trainingsdaten enthalten waren. In diesem Fall kann er auch Löschungen oder Korrekturen umsetzen oder umsetzen lassen, indem die entsprechenden Daten im ursprünglichen Datensatz entfernt oder korrigiert werden.

Wichtig ist jedoch, die Betroffenen darüber aufzuklären, dass diese Maßnahmen das bereits trainierte LLM und vom LLM verwendete Informationen nicht betreffen – sie wirken sich erst auf zukünftige Versionen des Modells aus, die mit den bereinigten Daten trainiert werden; dazu Ziffer 2.

KI-Betreiber sollten angemessene und wirksame technische, organisatorische und rechtliche Maßnahmen zur Unterstützung bei der Erfüllung von Betroffenenanfragen zu Trainingsdaten evaluieren und implementieren (lassen) wie Data-Lineage-Systeme zur Nachverfolgung von Datenquellen, Klassifizierungssysteme für personenbezogene Daten und strukturierte Datenkataloge, Named Entity Recognition zur Identifikation personenbezogener Daten und automatisierte Pseudonymisierungsverfahren. Diese sind je nach Situation auch mit den Anbietern der Trainingsdaten und/oder dem KI-Anbieter vertraglich zu regeln, insbesondere die Pflicht der Anbieter an sie weitergeleitete Betroffenenanfragen rechtzeitig zu beantworten.

2. Szenario: Personenbezogene Daten im LLM

Die Frage, ob ein trainiertes LLM selbst personenbezogene Daten im datenschutzrechtlichen Sinne enthält, ist in der Rechtswissenschaft und Praxis umstritten.

Wir vertreten hier die Tendenz, dass in den Modellparametern selbst keine personenbezogenen Daten im Sinne der DS-GVO enthalten sind, da die ursprünglichen Informationen vollständig transformiert und in abstrakten statistischen Mustern kodiert sind.

Egal wie man diese Frage beantwortet, die Erfüllung der Betroffenenrechte wie Auskunft, Löschung und Berichtigung im KI-Modell (LLM) ist technisch extrem schwer bis faktisch unmöglich. LLMs verfügen über Milliarden von Parametern, in denen Informationsfragmente verteilt und ohne direkte Zuordnungsmöglichkeit gespeichert sind. Es existiert keine eindeutige Abbildung zwischen den ursprünglichen Eingabedaten und den daraus resultierenden Modellparametern. Die emergenten Eigenschaften des Modells lassen sich nicht auf einzelne Trainingsdaten zurückführen. Die Parameter enthalten keine direkt identifizierbaren personenbezogenen Daten, sondern repräsentieren komplexe statistische Muster und Wahrscheinlichkeitsverteilungen. Es besteht keine technische Möglichkeit zur direkten Identifikation, ob und welche spezifischen personenbezogenen Daten im Modell enthalten sind. Personenbezogene Daten werden in der Regel erst durch spezifische Prompts oder Anfragen an das Modell sichtbar und erkennbar. Eine vollständige Inventarisierung aller im Modell potenziell gespeicherten personenbezogenen Daten ist technisch nicht realisierbar, da diese Information nicht explizit, sondern in verteilten Parametermustern kodiert ist.

Die isolierte Entfernung (Löschung) oder Änderung (Berichtigung) einzelner personenbezogener Informationen aus den Modellparametern ist mit aktuellen Technologien nicht möglich. Die gezielte Veränderung einzelner Parameter könnte zudem das gesamte Modellverhalten unvorhersehbar beeinträchtigen und zu einer Verschlechterung der Leistung auch in nicht betroffenen Bereichen führen.

Dies führt zu folgendem Umgang mit Betroffenenansprüchen:

Auskunftsrecht (Art. 15 DS-GVO):

Auskunft darüber, ob das KI-System oder Modell personenbezogene Daten des Betroffenen verarbeitet, können also faktisch nur mit »Nichtwissen/vielleicht ja/vielleicht auch nicht« beantwortet werden. Eine Kopie der Daten kann ebenfalls nicht zur Verfügung gestellt werden.

Auskunftsansprüche können/sollten daher mit Verweis auf Art. 11 Abs.2 DSGVO, Begründung und Erklärung der technisch nicht möglichen Erfüllung (unverhältnismäßiger Aufwand) beantwortet werden. Nach Art. 11 Abs.2 DS-GVO entfällt die Auskunftsverpflichtung, wenn der Verantwortliche den Betroffenen nicht identifizieren kann. Allerdings sollte (soweit möglich) eine Auskunft bzgl. der Trainingsdaten erfolgen (siehe oben).

Löschrecht (Art. 17 DS-GVO):

Der Anspruch auf Löschung personenbezogener Daten aus einem trainierten LLM ist aufgrund technischer Unmöglichkeit bzw. unverhältnismäßigen Aufwands in der Regel abzulehnen. Diese Ablehnung sollte detailliert begründet und dokumentiert werden, unter genauer Darlegung der technischen Limitationen.

Gleichzeitig sollte aber zugesichert werden, dass im Rahmen des technisch, operativ und vertraglich Möglichen und wirtschaftlich Sinnvollen beim nächsten Trainings-zyklus durch gezieltes Nachtraining eine faktische »Löschung« der Daten des Betroffenen angestrebt wird. Die Entwicklung effektiver Prompt-Filtering-Mechanismen kann ggf. ergänzend die gezielte Unterdrückung bestimmter Ausgaben ermöglichen, auch wenn die Information grundsätzlich im Modell verbleibt. Zudem muss eine konsequente Löschung der personenbezogenen Daten aus Trainingsdaten für künftige Modellversionen und -iterationen erfolgen, damit die betreffenden Informationen langfristig nicht mehr Teil des Modells sein werden.

Berichtigungsrecht (Art. 16 DS-GVO):

Auch der Anspruch auf Berichtigung personenbezogener Daten aus einem trainierten LLM ist aufgrund technischer Unmöglichkeit bzw. unverhältnismäßigen Aufwands in der Regel abzulehnen. Diese Ablehnung sollte detailliert begründet und dokumentiert werden, unter genauer Darlegung der technischen Limitationen.

Auch hier sollte im Rahmen des technisch, operativ und vertraglich Möglichen die Implementierung wirksamer Korrekturmechanismen durch gezielte Nachtrainings angekündigt werden, um falsche oder veraltete Informationen im Modell zu überschreiben. Die Entwicklung ausgereifter Überschreibungsmechanismen durch Prompt Engineering erlaubt die Korrektur von Ausgaben, auch ohne die Modell-parameter selbst zu verändern. Betroffene sollten aber darauf hingewiesen werden, dass bei jedem Berichtigungsversuch allerdings eine sorgfältige Abwägung zwischen der gewünschten Berichtigung und der Wahrung der Modellintegrität erfolgen muss. Hier widersprechen sich (leider) die Pflichten nach KI-VO und der DS-GVO. Die fortlaufende und lückenlose Dokumentation aller Berichtigungsmaßnahmen und ihrer Ergebnisse gewährleistet die notwendige Transparenz und Nachvollziehbarkeit.

3. Szenario: Personenbezogene Daten bei der Nutzung von KI-Systemen

Bei der Interaktion mit KI-Systemen teilen Nutzer häufig personenbezogene Daten in ihren Prompts mit. Dies ist problematisch, da KI-Systeme aus diesen Eingaben wieder lernen können. Die Differenzierung zwischen temporärer Verarbeitung und langfristiger Speicherung dieser Daten stellt eine zentrale Herausforderung dar. Oft fehlen wirksame Filter, die unbeabsichtigte oder sogar vorsätzliche Eingabe personenbezogener Daten verhindern könnten. KI-generierte Inhalte können zudem personenbezogene Daten reproduzieren oder durch Bias oder Halluzinationen falsche personenbezogene Daten erzeugen, die dann wieder zu berichtigen wären. Die Protokollierung von Nutzerinteraktionen erfolgt oft intransparent.

KI-Betreiber müssen aktiv sicherstellen, dass so wenig personenbezogene Daten wie möglich bei der Nutzung verarbeitet werden, insbesondere in Nutzereingaben (Prompts), da diese für weiteres Training verwendet werden könnten. Für alle dennoch verarbeiteten personenbezogenen Daten müssen ausreichende Rechtsgrundlagen vorliegen.

Wirksame automatisierte Erkennungs- und Filterungsmechanismen für personenbezogene Daten in Eingaben sollten implementiert werden, um unbeabsichtigte oder vorsätzliche Eingabe sensibler Daten zu erkennen und zu verhindern.

Besonderes Augenmerk muss auf die rechtskonforme Protokollierung und Dokumentation der Prompts gelegt werden. Nach entsprechenden Anfragen sollte eine umgehende und nachweisbare Löschung von Nutzerinteraktionen und generierten Inhalten erfolgen. Diese Nutzerinteraktionen und generierten Inhalten müssen gemäß rechtlicher Anforderungen für einen definierten Zeitraum aufbewahrt und anschließend gelöscht werden, um sowohl Betroffenenanfragen und Aufbewahrungspflichten erfüllen zu können als auch den Grundsatz der Speicherbegrenzung zu wahren. Eine genaue Dokumentation der Verarbeitungszwecke und Speicherfristen für diese Interaktionsdaten ist unerlässlich.

Profiling

Darüber hinaus regeln Art. 13 Abs.2 lit. f und Art. 14 Abs.2 lit. g DS-GVO besondere Informations-pflichten bei automatisierten Entscheidungen, insbesondere Profiling. In diesen Fällen hat das Unternehmen die betroffene Person über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling zu informieren und zudem aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person bereitzustellen. Dies kann Unternehmen speziell dann vor Schwierigkeiten stellen, wenn diese KI verwenden, die von anderen Anbietern entwickelt wurde und sie daher mitunter keine Kenntnis über die involvierte Logik haben.

Neben dem Informationsrecht sind auch im Rahmen des Auskunftsrechts der betroffenen Person gemäß Art. 15 Abs.1 lit. h DS-GVO zusätzliche Pflichten geregelt, wenn automatisierte Entscheidungsfindungen, einschließlich Profiling, durchgeführt werden. Betroffene können verlangen, detaillierte Informationen über die Logik, Reichweite und die beabsichtigten Auswirkungen solcher Verarbeitungen zu erhalten. Bei der Anwendung von KI kann das Bereitstellen präziser Informationen herausfordernd sein, besonders bei komplexen Datenverarbeitungsprozessen. Deshalb müssen Unternehmen gewährleisten, dass sie auch bei anspruchsvollen KI-gestützten Vorgängen in der Lage sind, klare und nachvollziehbare Informationen bezüglich der Datenverarbeitung zu vermitteln.

Artikel 24 ff. DS-GVO: Datenschutzrechtliche Verantwortlichkeit

Werden im Rahmen der Entwicklung, des Trainierens oder der Verwendung von KI-Modellen/KI-Systemen personenbezogene Daten verarbeitet, muss zunächst die datenschutzrechtliche Verantwortlichkeit für die jeweilige Datenverarbeitung geklärt werden. An diese Feststellung knüpfen dann die Pflichten und Rechtsfolgen aus den datenschutzrechtlichen Vorschriften an (Art. 24 DS-GVO). Die klare Zuordnung der Rollen ist essenziell, da sich hieraus die konkreten Pflichten (z. B. Informationspflichten, Gewährleistung von Betroffenenrechten, Abschluss von Verträgen) ergeben. Es können unterschiedliche Konstellationen von Verantwortlichkeiten vorliegen, die im Einzelfall sorgfältig zu prüfen sind:

Alleinige Verantwortlichkeit (Independent Controller)

Eine alleinige Verantwortlichkeit liegt vor, wenn ein Akteur allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO).

Ein **Beispiel** hierfür ist ein Unternehmen, das ein KI-System vollständig selbst entwickelt, trainiert und ausschließlich für eigene interne Zwecke nutzt, ohne Daten an Dritte weiterzugeben oder externe KI-Dienste maßgeblich einzubinden.[25]

Gemeinsame Verantwortlichkeit (Joint Controller)

Entscheiden hingegen zwei oder mehr Akteure gemeinsam über die Zwecke und Mittel der Verarbeitung, sind sie gemeinsame Verantwortliche nach Art. 26 Abs. 1 S. 1 DS-GVO. Die Rechtsprechung des EuGH legt diesen Begriff weit aus. Es ist dabei nicht erforderlich, dass jeder Beteiligte Zugang zu den personenbezogenen Daten hat. Es genügt vielmehr, wenn die Beteiligten durch gemeinsame Entscheidungen oder übereinstimmende Entscheidungen, die sich ergänzen, die Zwecke und Mittel der Verarbeitung festlegen. Eine gemeinsame Verantwortlichkeit kann bereits dann vorliegen, wenn ein Akteur durch die Bereitstellung einer Technologie (z. B. eines KI-Modells oder Plugins) die Verarbeitung ermöglicht und dabei (auch) eigene Zwecke verfolgt und Einfluss auf die Verarbeitung nimmt; ein wirtschaftliches Interesse kann dabei ausreichend sein. Im KI-Kontext ist gemeinsame Verantwortlichkeit daher insbesondere relevant, wenn mehrere Unternehmen gezielt zusammenwirken, um ein KI-Modell zu entwickeln oder zu trainieren, oder bei der Nutzung von KI-as-a-Service (KIaaS/LLMaaS) mit Anbieter-Optimierung. Setzt ein Unternehmen (Nutzer) ein von einem externen Anbieter bereitgestelltes KI-Modell ein und nutzt der Anbieter die bei der Nutzung anfallenden Daten (z. B. Prompts, Feedback) nicht nur im Auftrag des Nutzers, sondern auch für eigene Zwecke, insbesondere zur Verbesserung des KI-Modells für alle Kunden (tenant-übergreifende Optimierung), liegt regelmäßig eine gemeinsame Verantwortlichkeit vor, da der Anbieter ein Eigeninteresse verfolgt und durch die Gestaltung des Modells Einfluss auf die Mittel der Verarbeitung nimmt.

[25] LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0 vom 17.10.2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/ (zuletzt abgerufen am 23.05.2025).

Ähnlich kann bei der Einbindung von externen KI-Tools auf Webseiten (z. B. Chatbots) eine gemeinsame Verantwortlichkeit des Webseitenbetreibers mit dem Tool-Anbieter entstehen, wenn Daten an den Anbieter fließen und dieser sie auch für eigene Zwecke nutzt. Bei gemeinsamer Verantwortlichkeit müssen die Beteiligten gemäß Art. 26 Abs. 1 S. 2 DS-GVO in einer transparenten Vereinbarung festlegen, wer von ihnen welche Verpflichtungen gemäß der DS-GVO erfüllt.

Auftragsverarbeitung (Data Processor)

Verarbeitet ein Unternehmen personenbezogene Daten lediglich im Auftrag und streng nach Weisung eines Verantwortlichen, ohne eigene Zwecke zu verfolgen oder über die wesentlichen Mittel zu entscheiden, liegt eine Auftragsverarbeitung vor (Art. 4 Nr. 8, Art. 28 DS-GVO). Beispiele hierfür im KI-Kontext wären ein externer Dienstleister, der ein KI-Modell ausschließlich im Auftrag und nach genauen Vorgaben eines Unternehmens trainiert, oder die Nutzung eines Cloud-basierten KI-Systems, bei dem der Anbieter vertraglich und technisch sicherstellt, keinerlei eigene Nutzung der Daten vorzunehmen. Liegt eine Auftragsverarbeitung vor, muss zwischen dem Verantwortlichen und dem Auftragsverarbeiter ein Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO abgeschlossen werden.[26]

Die Verantwortlichkeiten können sich im Lebenszyklus eines KI-Systems ändern oder überlagern; daher müssen die Entwicklung, das Training, die Bereitstellung und die Nutzung/Anwendung eines KI-Systems separat betrachtet werden. Ein Akteur kann in einer Phase Auftragsverarbeiter sein und in einer anderen (Mit-)Verantwortlicher werden, beispielsweise wenn ein KIaaS-Anbieter die bei der Nutzung durch einen Kunden anfallenden Daten zur allgemeinen Modellverbesserung verwendet und somit zum gemeinsamen Verantwortlichen für diese spezifische Weiterverarbeitung wird.

Die korrekte Bestimmung der Verantwortlichkeit ist entscheidend, da eine Fehlklassifizierung zu DS-GVO-Verstößen führen kann. Unternehmen müssen ihre Analyse der Verantwortlichkeiten und die getroffenen Vereinbarungen (AVV, Art. 26-Vereinbarung) sorgfältig dokumentieren, um ihrer Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) nachzukommen.

Aus den Vorschriften der KI-VO zum »Quasi Provider« (Art. 25 KI-VO) ergeben sich ggf. ebenfalls Auswirkungen auf die datenschutzrechtliche Verantwortlichkeit. Art. 25 Abs 1 lit. c KI-VO regelt, dass Betreiber die den beabsichtigten Nutzungszweck des KI-Systems oder des Modells ändern oder substanzielle Änderungen daran vornehmen, wie ein Anbieter behandelt wird. Es ist schwer vorstellbar, dass eine Änderung des beabsichtigten Nutzungszwecks der KI nicht auch zu einer (mindestens gemeinsamen) datenschutzrechtlichen Verantwortlichkeit führt.

[26] LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0 vom 17.10.2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/ (zuletzt abgerufen am 23.05.2025).

Artikel 25 ff. DS-GVO: Privacy by Design/ Privacy by Default und Einsatz von geeigneten technischen und organisatorischen Maßnahmen

Im Zusammenhang mit KI erlangen die Konzepte »Privacy by Design« und »Privacy by Default« zunehmend an Bedeutung. Diese Ansätze sind nicht nur integraler Bestandteil der DS-GVO, sondern stellen auch einen zentralen Aspekt im Umgang mit personenbezogenen Daten innerhalb von KI-Systemen und Modellen dar. Der folgende Abschnitt befasst sich mit der Anwendung dieser Prinzipien im Kontext von KI und beleuchtet die Rolle geeigneter technischer und organisatorischer Maßnahmen (TOM) zur Gewährleistung des Datenschutzes.

»Privacy by Design« bezeichnet einen Ansatz, bei dem Datenschutz bereits in der Entwicklungsphase von Produkten und Systemen berücksichtigt wird. »Privacy by Default« hingegen sichert durch die Umsetzung datenschutzfreundlicher Voreinstellungen, dass standardmäßig nur die für den jeweiligen Zweck notwendigen personenbezogenen Daten verarbeitet werden. Beide Konzepte sind in Art. 25 DS-GVO verankert und verpflichten Entwickler und Anbieter von KI-Systemen, Datenschutz von Anfang an in ihre Systeme und Prozesse zu integrieren.

Die Implementierung geeigneter TOM ist essenziell, um den Anforderungen des Datenschutzes in KI-Systemen und Modellen gerecht zu werden. Bei der Auswahl der Maßnahmen sind Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die aus der Verarbeitung hervorgehenden Risiken für die betroffenen Personen und der Stand der Technik zu berücksichtigen. Umgesetzte TOM sollten kontinuierlich überprüft und ggf. angepasst werden, um aktuellen Risiken und technologischen Entwicklungen Rechnung zu tragen.

Beispielhaft bieten sich als Maßnahmen zur Datenminimierung unter anderem vorgeschaltete Prompt-Filter oder vergleichbare Technologien zur Einschränkung/ Standardisierung des Inputs an, um die Eingabe personenbezogener Daten so weit wie möglich zu verhindern. Weiterhin sollten Beschäftigte mittels Schulungen und Informationsmaterial dabei unterstützt werden, ihre Eingaben in die KI-Anwendung möglichst datensparsam gestalten zu können. Hinweise und Regelungen zur (Nicht-) Eingabe personenbezogener Daten in KI-Anwendungen können auch in Form von Nutzungsbedingungen, Richtlinien oder einem Verhaltenskodex geregelt werden.

Die Erstellung pseudonymisierter Benutzeraccounts und die Anonymisierung der in das KI-System oder dem Modell eingehenden Daten, dient weiterhin dem Ziel der Datenminimierung.

Um die Einhaltung der Zweckbindung sicherzustellen, sollte mit dem Anbieter vertraglich ausgeschlossen werden, dass die in die KI-Anwendung eingegebenen Daten zum weiteren Training der KI durch den Anbieter weiterverarbeitet werden. In manchen Anwendungen kann dies auch über entsprechende Konfigurationsmöglichkeiten technisch umgesetzt werden, genauso wie ein Opt-Out aus dem anwendungsseitigen Anlegen eines Nutzungsverlaufs. Falls solche Einstellungen nur auf Nutzerebene vorgenommen werden können, sollten die Nutzerinnen und Nutzer entsprechend instruiert werden. Weiterhin sollte sichergestellt sein, dass die mit der KI

erzeugten Inhalte, sofern sie personenbezogene Daten enthalten, nur nach dem Need-to-know-Prinzip verarbeitet werden.

Für den Einsatz von KI-Anwendungen liegt bei der Umsetzung von TOM eine Herausforderung darin, dass bei den unterschiedlichen auf dem Markt verfügbaren Einsatzformen von KI (z. B. »KI as a Service«, öffentlich verfügbare Systeme oder individuell erstellte/angepasste Systeme) unterschiedlicher Spielraum für das Ergreifen eigener Maßnahmen seitens des Verantwortlichen besteht. So wird in der Regel bei selbst oder spezifisch im Auftrag erstellten KI-Anwendungen auch umfangreiches Customizing möglich sein, während bei der Nutzung eines allgemein z. B. per Browser aufrufbaren Standardprodukts kaum Einfluss auf die technische Gestaltung genommen werden kann. Entsprechend sind je nach Anwendung unterschiedliche technische Maßnahmen aufseiten des Verantwortlichen umsetzbar oder ggf. nicht umsetzbar. Organisatorische Maßnahmen sind von dieser Variabilität weniger betroffen, wodurch der Verantwortliche sie weitgehend eigenständig und unabhängig von der konkreten Anwendung implementieren kann.

Bei Einsatzformen von KI-Systemen und Modellen, die es einsetzenden Unternehmen nicht ermöglichen, technische Maßnahmen in der Anwendung selbst umzusetzen, sollten – insbesondere mit Blick auf die Transparenz – zumindest entsprechende Hinweise implementiert werden. Dies kann z. B. bei der Nutzung allgemein verfügbarer online KI-Anwendungen auf dienstlichen Endgeräten durch eine in den Browser integrierte Warnung erfolgen, in der bei Besuch einer entsprechenden Website auf bestehende Acceptable Use-Richtlinien, Betriebsvereinbarungen o. Ä. hingewiesen wird. Über die Risiken der Nutzung solcher KI-Anwendungen, mit deren Anbietern in der Regel gerade keine gesonderten vertraglichen Vereinbarungen bzgl. Vertraulichkeit, Zweckbindung etc. bestehen, sollten die Nutzer unabhängig davon auch mittels Schulungen und Informationsmaterial sensibilisiert werden.

Letztendlich bemisst sich der Umfang und die Auswahl der zu ergreifenden TOM an den mit dem konkreten Use Case verbundenen Risiken und Umständen, muss also stets in einer Einzelfallbetrachtung ermittelt werden. Neben den hier beispielhaft

genannten eher KI-spezifischen Maßnahmen sind dabei auch zur grundsätzlichen Gewährleistung der Datensicherheit in IT-Systemen eingesetzte TOM, z. B. Verschlüsselung und Zugriffskontrollen, zu berücksichtigen. Wo dem Verantwortlichen selbst die Implementierung insbesondere technischer Maßnahmen vor dem oben dargestellten Hintergrund nicht ausreichend möglich ist, muss auf andere Weise (z. B. vertraglich mit dem Anbieter) sichergestellt werden, dass trotzdem ein angemessenes Schutzniveau sichergestellt ist.

Die Integration von »Privacy by Design« und »Privacy by Default« in KI-Systeme oder Modelle sowie die Implementierung geeigneter TOM sind nicht nur rechtliche Erfordernisse, sondern tragen auch zur Vertrauensbildung bei Nutzenden und zur Förderung ethischer Standards in der Technologie bei. Ein einheitliches Ordnungsschema zur Identifikation und Umsetzung relevanter technischer und organisatorischer Maßnahmen hinsichtlich Privacy by Design und Sicherheit der Verarbeitung bietet das vom Bitkom erstellte Datenschutz-Reifegradmodell zur

Abbildung von technisch-organisatorischen Maßnahmen bei der Auftrags-verarbeitung.[27]

Artikel 30 DS-GVO: Aufnahme der Verarbeitung in das Verzeichnis von Verarbeitungstätigkeiten

Sollten personenbezogene Daten mithilfe einer KI verarbeitet werden, so sind diese Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO in einem Verzeichnis von Verarbeitungstätigkeiten zu hinterlegen.

Details zur Definition eines solchen Verarbeitungsverzeichnisses, zu Grundlagen sowie zum Prozess zur Erstellung einer solchen Dokumentation finden Sie im Bitkom-Leitfaden »Das Verarbeitungsverzeichnis«[28].

Hier besteht die Gefahr von intransparenter Dokumentation. Diese Intransparenz tritt aufgrund von ungenauen Angaben in Bezug auf die Verarbeitung der Daten der einzelnen KI-Anwendungen auf. Oft ist unklar, wie, wozu und wie lange die verwendeten Daten auf Servern von KI-Anbietern verarbeitet werden. Hierbei handelt es sich um eine »Black Box«, die sich aufgrund von selbstlernenden und komplexen Strukturen bildet.

Um dieser Intransparenz entgegenzuwirken, sollten Kontrollmaßnahmen festgehalten werden, die detaillierte Informationen über die Verarbeitung der Daten sicherstellen, damit eine präzise Dokumentation des Verzeichnisses von Verarbeitungstätigkeiten gewährleistet werden kann. Solche Kontrollmaßnahmen können bspw. darin bestehen, dass die Dokumentation im Rahmen der Anschaffung des KI-Modells im Verarbeitungsverzeichnis hinterlegt wird.

Artikel 33, 34 DS-GVO: Prozess Datenschutzvorfall

Der Datenschutzvorfall-Prozess beim Einsatz von KI unterscheidet sich grundsätzlich nicht vom allgemeinen Vorgehen bei einer DSV (Datenschutzverletzung). Besonderes Augenmerk ist auf die Analysephase und den Faktor Zeit zu legen, Details s. u. Herausforderungen.

Allgemeine Informationen hinsichtlich der Verletzung des Schutzes personenbezogener Daten im Sinne der DS-GVO, einer ggf. notwendigen Meldung und Benachrichtigung betroffener Personen, sowie zur Auslegung der Art. 33 und 34 DS-GVO sind im Bitkom-Leitfaden Datenschutzverletzung und Meldung im Kontext des

[27] Bitkom e.V, Datenschutz-Reifegradmodell zur Abbildung von technischen und organisatorischen Maßnahmen bei der Auftragsverarbeitung, 2024, abrufbar unter: . 241104-LF-Datenschutz-Reifegradmodell-Bitkom.pdf (zuletzt abgerufen am 23.05.2025).
[28] Bitkom e.V. , Das Verarbeitungsverzeichnis , Leitfaden 2017, abrufbar unter: https://www.bitkom.org/sites/main/files/file/import/180529-LF-Verarbeitungsverzeichnis-online.pdf (zuletzt abgerufen am 23.05.2025).

»Hafnium Hacks«[29] dargestellt. Dort finden sich auch Ausführungen zu Auswirkungen auf eine Auftragsverarbeitung.

Anwendungsfälle

Beim Einsatz von KI sind insbesondere folgende **Use Cases** im Kontext von Datenschutzvorfällen vorstellbar:

- **Anwendungsfall 1:** Weiterverbreitung oder Veröffentlichung von personenbezogenen Daten durch KI-Systeme und Modelle ohne Wissen und ohne Rechtsgrundlage (Verstoß gegen Grundsatz der Transparenz, Rechtmäßigkeit)
- **Anwendungsfall 2:** KI funktioniert nicht ordnungsgemäß – Softwarefehler in KI-Lösung verursacht eine unbefugte Offenbarung personenbezogener Daten von Nutzerinnen und Nutzer
  - Beispiel: im Beschäftigtenkontext werden Daten wegen fehlerhafter KI mit Kolleginnen und Kollegen geteilt, die keine Zugriffsberechtigung besitzen
- **Anwendungsfall 3:** KI-gesteuerter Hackerangriff auf ein Unternehmen, bei dem personenbezogene Daten z. B. von Kundinnen und Kunden oder Beschäftigten kompromittiert werden
  - Beispiel: Ein KI-gesteuertes Chatbot-System könnte von einem Angreifer gehackt werden, der dann gefälschte Unterhaltungen führt, um persönliche Informationen von Nutzern zu stehlen, indem er sich als legitimer Service ausgibt.
- **Anwendungsfall 4:** Kompromittierung von personenbezogenen Daten bei Vorgängen ohne menschliche Kontrolle bzw. Interaktion mit direkten rechtlichen Auswirkungen auf betroffene Personen z. B. im Rahmen von automatisierten Entscheidungsfindungen oder KI-gestütztem Scoring
  - Beispiel 1: Anwendung für Bonitätsrating/Kreditvergabe
  - Beispiel 2: Ein Bewerbungs-Tracking-System, das auf KI basiert, könnte aufgrund von Voreingenommenheit in den Trainingsdaten Bewerberinnen und Bewerber bestimmter ethnischer Gruppen benachteiligen, indem es sie fälschlicherweise ausschließt.

Hinweis: Kommt der Verantwortliche bei der Analyse zu dem Ergebnis, dass die DSV voraussichtlich ein hohes Risiko für Rechte und Freiheiten der Betroffenen zur Folge hat, muss er diese gemäß Art. 34 Abs.1DS-GVO unverzüglich von der Verletzung benachrichtigen.[30]

[29] Bitkom e.V, Datenschutzverletzung und Meldung im Kontext des »Hafnium Hacks«, Leitfaden, 2017abrufbar unter: Datenschutzverletzung und Meldung im Kontext des "Hafnium Hacks" (zuletzt abgerufen am 23.05.2025).
[30] Zu Modalitäten und Inhalt einer Benachrichtigung s. Art. 34 Abs. 1 und 2 DS-GVODS-GVO, zu Ausnahmen s. Art. 34 Abs 3 DS-GVO. Details s. Bitkom-LF aaO, vgl. Fn. 15.

Herausforderungen

Bei der Beurteilung von Datenschutzvorfällen in Verbindung mit KI gibt es spezifische Herausforderungen, welche den nachfolgenden Aspekten zugeordnet werden können:

- **Feststellung einer Datenschutzverletzung:** Zu Transparenzanforderungen in Verbindung mit KI (Siehe die Ausführungen im Abschnitt Transparenz- und Informationspflichten auf Seite 36.) Aufgrund der technischen Komplexität von KI leidet die Nachvollziehbarkeit ihrer Funktionsweise. Verantwortlichen fehlt häufig das nötige technische Verständnis. Dieses ist jedoch wichtig, um beurteilen zu können, ob KI ordnungsgemäß funktioniert. Die hohe Komplexität von KI-Systemen oder Modellen erschwert zudem die Risikoeinschätzung im Einzelfall. Die Feststellung, ob überhaupt eine Verletzung der Sicherheit und damit eine meldepflichtige Datenschutzverletzung vorliegt, kann somit in der Praxis herausfordernd sein. Oft sehen sich Verantwortliche mit intransparenten und wenig verständlichen Informationen der KI-Hersteller konfrontiert. Wichtig dabei ist, im Einzelfall zu untersuchen, welche personenbezogenen Daten konkret z. B. für ein Training von Systemen verwendet werden. Diese Analyse sollte bestenfalls schon im Rahmen der Dokumentation für das Verzeichnis von Verarbeitungstätigkeiten i. S. v. Art. 30 DS-GVO geschehen – bevor es zu einem Vorfall kommt.

- **Verantwortlichkeit:** Der Aspekt der datenschutzrechtlichen Verantwortlichkeit kann bei einer DSV vor dem Hintergrund der gesetzlichen 72h-Stunden-Frist besonders herausfordernd werden. Es wird daher empfohlen, diese Frage frühzeitig zu klären, bevor es zu einer Datenschutzverletzung kommt. An dieser Stelle wird auf die Verpflichtung zur unverzüglichen Meldung von Auftragsverarbeitern gegenüber dem Verantwortlichen gemäß Art. 33 Abs.2 DS-GVO hingewiesen[31].

- **Faktor Zeit:** Bei Datenschutzverletzungen ist vor dem Hintergrund der strengen gesetzlichen Anforderungen (72-Stunden-Meldefrist für Verantwortliche, »unverzüglich« für Auftragsverarbeiter) besonders wichtig, nach Bekanntwerden unverzüglich mit einer Analyse zu beginnen. Denn im Zusammenhang mit KI sind mögliche Folgen für die Datensicherheit aufgrund der Komplexität der KI (z. B. wo kommen die Daten der KI her) (s. o.) schwerer abschätzbar als in Szenarien ohne KI. Hilfreich ist die Möglichkeit nach Art. 33 Abs.4 DS-GVO bzgl. eines schrittweisen Vorgehens, wenn Informationen nicht zur gleichen Zeit bereitgestellt werden können. Dann können diese schrittweise der zuständigen Aufsichtsbehörde zur Verfügung gestellt werden.

- **Fehlende Praxisfälle und unterschiedliche Positionierung der Datenschutz-Aufsichtsbehörden:** Angesichts der rasanten Entwicklung der KI-Thematik stehen Verantwortliche (Unternehmen) mit ihren Erfahrungen zu Datenschutz-verletzungen noch am Anfang. Herausfordernd ist auch die unterschiedliche Definition und Positionierung von Datenschutz-Aufsichtsbehörden von bzw. zu KI per se. Mit zunehmender praktischer Erfahrung seitens der Verantwortlichen und spezifischer Hilfestellungen seitens der Datenschutz-Aufsichtsbehörden konkret zum Thema Datenschutzverletzung bei KI-Nutzung werden Verantwortliche und Auftragsverarbeiter mehr Orientierung und Rechtssicherheit erhalten.

[31] Details s. Bitkom-Leitfaden, aaO, s. Fn. 15.

- Praktische Hilfestellung im Vorfeld bzw. bei der Analyse von Datenschutzvorfällen bieten folgende Fragestellungen:
- Integration von KI: Auf welche Art wurde die KI integriert?
- Beispiel: sog. »model serving« oder »model training«?
- Reichweite: Ist die KI-Anwendung nach »außen« exponiert, i. S. v. öffentlich zugänglich?
- Technische und organisatorische Maßnahmen (TOM):
  - Welche technischen und organisatorischen Maßnahmen müssen ergriffen werden, um sicherzustellen, dass personenbezogene Daten im Rahmen der Eingabe oder dem Abruf von Ergebnissen vor unbefugter Offenlegung, Veränderung oder Verlust der Verfügbarkeit geschützt sind?
  - Beispiele für TOM: KI-Governance, Privacy-by-design/default, Pseudonymisierung, Anonymisierung, Verschlüsselung, sichere Speicherung, usw.
  - Greifen die Schutzmaßnahmen wie geplant?
- Vertragliche Aspekte:
  - Bei Beschaffung von Generativer KI wird empfohlen, die Vertragsbedingungen sorgfältig zu prüfen, unter denen ein KI-System oder Modell erworben bzw. lizenziert wird. Ist der Umgang mit Datenschutzverletzungen geregelt und insbesondere welche Vertragspartei trägt welche Pflichten?

Artikel 35 DS-GVO: Durchführung einer Datenschutzfolgenabschätzung/ Folgenabschätzung

Nach der KI-Verordnung ist vor Einführung oder Nutzung von Hoch-Risiko-Systemen und General-Purpose-KI-Modellen und Systemen mit systemischen Risiken ein »fundamental rights impact assessment« (»FRIA«) (Grundrechtsfolgenabschätzung) durchzuführen. Diese Folgenabschätzung ist mit einer Datenschutz-Folgenabschätzung (DSFA) nach DS-GVO nicht identisch, sondern eine **zusätzliche** Anforderung der KI-VO.

Beim Einsatz von KI spielt das Thema DSFA eine große Rolle, da die Verwendung von KI-Systemen und Modellen angesichts einer potenziellen Diskriminierungsgefahr sowie fehlender Kontrollmöglichkeiten mit hohen Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden sein kann.

Allgemeine Ausführungen zum Thema DSFA sowie zum Vorgehen bei der Prüfung der Pflicht zur Durchführung einer DSFA enthält der Bitkom-Leitfaden **»Risk Assessment & Datenschutz-Folgenabschätzung«**[32].

[32] Bitkom e.V., Risk Assessment & Datenschutz-Folgenabschätzung, s. Risk Assessment & Datenschutz-Folgenabschätzung , Leitfaden 2017 , abrufbar unter: Auftragsverarbeitung , (zuletzt abgerufen am 23.05.2025).

Erforderlichkeit einer DSFA/FRIA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge (**»Schwellwertanalyse«**). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Bei der Bewertung des konkreten Risikos muss zunächst die Auswirkung der gesetzlichen Kategorisierung von KI-Systemen nach der KI-VO (Art. 6, Annex II) berücksichtigt werden. Wenn KI-Systeme bereits nach der KI-VO als Hochrisikosystem gelistet/angesehen werden, ist recht unwahrscheinlich, dass die gleichen Systeme rein datenschutzrechtlich zu keinem hohen Risiko führen.

Im Rahmen der FRIA werden u. a. auch datenschutzrelevante Aspekte geprüft, wie:

- Kategorien von natürlichen Personen und Gruppen, die von der Nutzung des Systems betroffen sein könnten
- Vereinbarkeit der Nutzung des Systems mit den einschlägigen Rechtsvorschriften der Union und der Mitgliedstaaten über die Grundrechte (= DS-GVO)
- die nach vernünftigem Ermessen vorhersehbaren Auswirkungen des Einsatzes des Hochrisiko-KI-Systems auf die Grundrechte
- spezifische Schadensrisiken, die sich auf marginalisierte Personen oder schutzbedürftige Gruppen auswirken können

Daher ist ebenfalls unwahrscheinlich, dass FRIA und DFSA bei den Risiken zu erheblich abweichenden Ergebnissen kommen.

Art. 35 Abs.3 DS-GVO benennt – nicht abschließend vgl. »insbesondere« – einige Faktoren, die wahrscheinlich zu einem hohen Risiko i.S.d. Art. 35 Abs.1 DS-GVO und damit zu einer entsprechenden Pflicht zur Durchführung einer DSFA führen:

a. 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;

b. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs.1 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art.10 DS-GVO oder

c. systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Die DSK hat eine **Muss-Liste** der Verarbeitungsvorgänge i.S.v. Art. 35 Abs. 4 S. 1 DS-GVO erstellt, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (sogenannte »Blacklist«)[33]. Diese nimmt in Ziff. 11 explizit Bezug auf den Einsatz von KI:

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
11	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 ein, welches mit Kunden durch Konversation interagiert und für deren Beratung personenbezogene Daten durch eine künstliche Intelligenz verarbeitet werden.

Die Liste ist nicht abschließend, sondern ergänzt die in den Absätzen 1 und 3 des Arti. 35 DS-GVO enthaltenen allgemeinen Regelungen. Die Liste orientiert sich wiederum an der allgemeinen Vorgehensweise wie beschrieben in Arbeitspapier 248 Rev. 1 der früheren Artikel 29-Gruppe[34] und ergänzt und konkretisiert diese.

Von der Möglichkeit, entsprechende **Braucht-Nicht-Listen** ohne DSFA-Pflicht gemäß Art. 35 Abs.5 DS-GVO zu erstellen (»Whitelists«), haben die deutschen Aufsichtsbehörden bislang keinen Gebrauch gemacht.

Vorherige Konsultation der Aufsichtsbehörde gemäß Art. 36 DS-GVO

Kommt der Verantwortliche bei der Durchführung einer DSFA zu dem Ergebnis, dass seine geplante Verarbeitung im Rahmen der Nutzung von KI ein hohes Risiko zur Folge hätte, muss er vor der Verarbeitung die Aufsichtsbehörde konsultieren, soweit er keine Maßnahmen zur Eindämmung des Risikos trifft.

Pflicht zur DSB-Benennung gemäß § 38 BDSG

Bei positiver Feststellung einer DSFA-Pflicht beim Einsatz von KI ist die nach § 38 I 2 BDSG resultierende Verpflichtung zur Benennung eines bzw. einer Datenschutzbeauftragen (DSB) zu beachten – und zwar unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen[35]. Die Benennungspflicht richtet sich sowohl an

[33] DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Kurzpapier vom 17.10.2018, abrufbar unter: Offizielles Kurzpapier der DSK, (zuletzt abgerufen am 23.05.2025).
[34] Datenschutzgruppe nach Artikel 29 (ersetzt durch EDSA seit 25.05.2018); vgl. Arbeitspapier 248 Rev. 1 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«, s. wp248 rev.01_de, abrufbar unter: Datenschutzkonferenz (datenschutzkonferenz-online.de)(zuletzt abgerufen am 23.05.2025).
[35] Vgl. § 38 Abs. 1 Satz 1 BDSG »...in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen«.

Verantwortliche als auch an Auftragsverarbeiter und kann für diese eine Herausforderung darstellen.

Dies kann in der Praxis beispielsweise in folgenden Szenarien relevant sein:

Beispiel: Der Einsatz von KI-basierten Lösungen durch Verantwortliche, die selbst nicht Anbieter der Lösung sind, jedoch Produkte nutzen, in denen KI verbaut ist. Allein die Nutzung kann eine DSFA-Pflicht auslösen und damit zwangsweise die Bestellung eines DSB.

Beispiel: Die Nutzung von Online-Office-Suiten durch KMU.

Die vorgenannte, nationale Regelung steht in der Kritik. So hat sich u. a. Bitkom im Rahmen des Konsultationsprozesses zum geplanten BDSG-Änderungsgesetz des BMI im Jahr 2023 für eine Streichung von § 38 I 2 1. Fall BDSG ausgesprochen, um das Datenschutzrecht mit dem Recht auf unternehmerische Freiheit in eine angemessene Balance zu bringen, eine Gleichbehandlung von Verantwortlichen in der EU und Wettbewerbsgleichheit sicherzustellen sowie innovative Geschäftsmodelle im Zuge der digitalen Transformation zu unterstützen.[36] Bitkom wird das Gesetzgebungsverfahren zur BDSG-Änderung weiter beobachten.

Ergänzend wird auf die Notwendigkeit zusätzlicher Prüfungen beim Einsatz von Künstlicher Intelligenz gemäß der KI-Verordnung hingewiesen.

Fazit DSFA

Werden mithilfe von KI rein automatisierte Entscheidungen getroffen bzw. vorbereitet oder erfolgt eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, führt die Schwellwertanalyse in der Regel zu dem Ergebnis, dass eine Datenschutz-Folgenabschätzung gem. Artikel 35 DS-GVO durchgeführt werden muss.

Besonders die Beurteilung der Risikolage kann in der Praxis herausfordernd sein, da Verantwortliche oftmals keine bzw. nicht hinreichend Transparenz zu Verarbeitungsdetails, verwendeten Algorithmen und involvierter Logik haben. Diese Herausforderung besteht ebenfalls, wenn KI-Anwendungen im Rahmen einer Auftragsverarbeitung genutzt werden. Hier sind Verantwortliche auf die entsprechenden Informationen der Hersteller angewiesen, um ihren datenschutzrechtlichen Verpflichtungen nachkommen zu können. Details zum Aspekt Transparenz und Informationspflichten s. o.

In der unternehmerischen Praxis zeigt sich, dass gerade bei KI-Projekten ein großer Zeitdruck besteht, da sich Unternehmen mit einer schnellen Realisierung Wettbewerbsvorteile sichern möchten. Verantwortlichen wird daher empfohlen, sich frühzeitig mit der Frage bzgl. Durchführung einer DSFA auseinanderzusetzen, zumal diese vor dem Start der Verarbeitung personenbezogener Daten erfolgen muss.

Da die Durchführung einer DSFA inklusive Erstellung eines DSFA-Berichts einer Vorbereitung bedarf und zeitlich aufwändig ist, wird geraten, entsprechend Vorlaufzeit einzuplanen. Erfahrungswerte aus der unternehmerischen Praxis liegen im Bereich von

[36] Bitkom e.V., Stellungnahme zum BDSG-Änderungsgesetz, Stellungahme 2023, abrufbar unter: https://www.bitkom.org/Bitkom/Publikationen/Bundesdatenschutzgesetz-2023 (zuletzt abgerufen am 23.05.2025).

ca. 3 bis 6 Monaten Dauer je Vorhaben und abhängig von der Komplexität im Einzelfall. Eine ggf. nötige Konsultation der Aufsichtsbehörde verlängert den Prozess.

Weiterführende Informationen zu DSFA in Verbindung mit KI sowie zu DSFA allgemein

- Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI[37]
- Hambacher Erklärung der DSK zur Künstlichen Intelligenz[38]
- DSK-Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO[39] mit allgemeinen Ausführungen zur DSFA-Thematik.
- Bitkom Leitfaden Risk Assessment & Datenschutz-Folgenabschätzung[40]

Berechtigungskonzept

Ein Berechtigungskonzept für KI ist ein wichtiger Baustein für den verantwortungsvollen und rechtskonformen Einsatz von KI-Anwendungen. Es sollte die Anforderungen und Besonderheiten von KI berücksichtigen und die Rollen, Rechte und Pflichten der beteiligten Akteure klar regeln.

Insbesondere folgende Fragen bieten u. a. eine Hilfestellung:

- Muss der Datenzugriff auf einen bestimmten Personenkreis, z. B. Administratoren, beschränkt werden?
- Welche Vertraulichkeit haben die im KI-System oder Modell verarbeiteten personenbezogenen Daten?
- Welche Rolle spielt eine Zugangskontrolle (z. B. Authentifizierungssystem)?

Löschkonzept

Die Verarbeitung personenbezogener Daten durch KI-Systeme und Modelle stellt Unternehmen vor praktische Herausforderungen und wirft spezifische Fragen auf, die im Rahmen eines Löschkonzepts berücksichtigt werden müssen. Ein Aspekt dabei ist, ob innerhalb eines KI-Modells bzw. eines LLM gelöscht werden kann.

Die Beantwortung dieser Frage hängt initial von der Frage ab, ob ein KI-Modell personenbezogene Daten enthalten kann. Während der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die Position vertritt, dass in Large Language Modellen (LLM) bei technischer Betrachtung keine personenbezogenen Daten gespeichert werden, kommt der EDSA zu einer gegenteiligen Auffassung, dass keine

[37] DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, Stand: 06.11.2019, abrufbar unter: 20191106_positionspapier_kuenstliche_intelligenz.pdf (zuletzt abgerufen am 23.05.2025).
[38] Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Hambacher Schloss 3. April 2019, Hambacher Erklärung zur Künstlichen Intelligenz, Sieben datenschutzrechtliche Anforderungen, vgl. Ziff. 6; Link s. 20190405_hambacher_erklaerung.pdf (datenschutzkonferenz-online.de).
[39] DSK, Kurzpapier Nr.5 Datenschutz- Folgenabschätzung nach Art. 35 DS-GVO, Stand: 17.12.2018, abrufbar unter: DSK_KPNr_5_Datenschutz-Folgenabschätzung_Lizenzvermerk, (zuletzt abgerufen am 23.05.2025).
[40] s. o. Fn. 1.

automatische Anonymität in KI-Modellen gegeben sei. Aus Sicht des EDSA müssen Unternehmen sicherstellen, dass sie über klare Löschkonzepte verfügen und geeignete technische und organisatorische Maßnahmen ergreifen, um das Recht auf Löschung effektiv umzusetzen.

KI-Systeme und Modelle nutzen oft komplexe und verteilte Speichersysteme, einschließlich Cloud-basierter Dienste. Diese Systeme können die Lokalisierung und Löschung von Daten erschweren, insbesondere wenn Daten über verschiedene Standorte und Jurisdiktionen hinweg gespeichert werden. Ein effektives Löschkonzept muss daher die spezifischen Speicherstrukturen und Zugriffsmechanismen berücksichtigen, die in KI-Systemen und Modellen verwendet werden.

Das Recht auf Vergessenwerden (Art. 17 DS-GVO) ermöglicht es Einzelpersonen, die Löschung ihrer personenbezogenen Daten unter bestimmten Umständen zu fordern. Eine KI muss in der Lage sein, solche Anforderungen effizient und vollständig umzusetzen.

Automatisierte Löschmechanismen können eingerichtet werden, um Daten nach Ablauf ihrer Relevanz oder auf Anfrage automatisch zu löschen.

Es ist wichtig, den Prozess der Datenlöschung zu dokumentieren, um die Einhaltung von Datenschutzbestimmungen nachzuweisen. Dies ist wichtig, um bei Anfragen von Datenschutzbehörden oder betroffenen Personen Rechenschaft ablegen zu können.

Interne Richtlinien zur Nutzung von KI

Unternehmen, die sich mit der Nutzung von KI befassen, müssen zunächst vielfältige technische, kommerzielle und rechtliche Bewertungen und Festlegungen der internen und externen Anforderungen an die KI durchführen.[41] Dazu gehört auch die Erstellung einer unternehmensinternen Richtlinie zur Nutzung von (generativer) KI[42]. Datenschutzrechtliche Aspekte müssen bei der Entwicklung, Implementierung und Nutzung von KI-Systemen bzw. Modellen eine zentrale Rolle spielen. Die Richt-linien sollten sicherstellen, dass personenbezogene Daten rechtmäßig und zweckgebunden erhoben, verarbeitet und bei Dateneingaben und -ausgaben auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Es sollten – soweit nötig – Maßnahmen ergriffen werden, um die Datensicherheit zu gewährleisten, wie beispielsweise die Anonymisierung oder Pseudonymisierung von Daten. Die Richtlinie sollte einen Prozess zur Erfüllung der gegebenenfalls bestehenden Rechte der betroffenen Personen, wie das Recht auf Information, Berichtigung und Löschung beinhalten. Zudem sollten die Richtlinien sicherstellen, dass die KI-Systeme und Modelle auch aus Sicht der Verarbeitung personenbezogener Daten transparent und erklärbar sind, um den Schutz der Privatsphäre und die Wahrung der Rechte der betroffenen Personen zu gewährleisten.

[41] Bitkom e.V., Generative KI im Unternehmen, Leitfaden 2025, Kapitel 2.2, abrufbar unter: https://www.bitkom.org/sites/main/files/2024-02/Bitkom-Leitfaden-Generative-KI-im-Unternehmen.pdf (zuletzt abgerufen am 23.05.2025).
[42] Bitkom e.V., Generative KI im Unternehmen, Leitfaden 2025, Kapitel 3.5.5, abrufbar unter: https://www.bitkom.org/sites/main/files/2024-02/Bitkom-Leitfaden-Generative-KI-im-Unternehmen.pdf (zuletzt abgerufen am 23.05.2025).

Warum ist das wichtig? Unternehmen haben dadurch die Chance, zugleich die Rechenschafts- und Nachweispflicht aus der DSGVO (z. B. Art. 5 Abs. 2, Art. 30 DS-GVO) sowie die Anforderungen der KI-VO (z. B. Art. 9, 11, 27 KI-VO) zu erfüllen. Außerdem lassen sich Bußgelder vermeiden (Art. 83 Abs. 5 lit. a DSGVO, Art. 99 ff. KI-VO).

Praxistipp:

- Synergieeffekte nutzen: Prüfen Sie, inwieweit Nachweise nach KI-VO (z. B. technische Dokumentation nach Art. 11 i. V. m. Anhang IV) auch als Nachweise nach DSGVO verwendet werden können (z. B. für das Verzeichnis der Verarbeitungstätigkeiten oder TOM nach Art. 32 DSGVO).
- Wichtig ist es auch, von Anfang an eine Dokumentation von KI-Modellen und Systemen, Tools und Anwendungsfällen sicherzustellen, damit ausreichend Klarheit besteht und nicht zu einem späteren Zeitpunkt erst mühsam begonnen werden muss, den KI-Bestand im Unternehmen zu ermitteln und die jeweiligen Risiken im Einzelnen zu bewerten.

Zu berücksichtigen ist auch die Vielfalt der Technologien und Anwendungsfelder, die Schnelligkeit der Entwicklung und der notwendige Detaillierungsgrad. Es wird sich daher oft empfehlen, eine generelle und ggf. abstrakte Richtlinie (Policy) durch detailliertere Vorgaben zu ergänzen, die einzelne Aspekte eingehender regeln. Die weiteren Regelungen (z. B. »Standards«) bieten dann die Flexibilität, einzelne Aspekte nicht nur spezifisch zu regeln, sondern auch die Regeln bei Bedarf zu aktualisieren, ohne stets die grundlegende Richtlinie neu fassen und publizieren zu müssen. Der Zuschnitt dieser detaillierten Regelungen kann nicht allgemeingültig empfohlen werden, sondern ergibt sich aus Art und Umfang der KI-Nutzung im Unternehmen. Werden z. B. eigene Modelle oder Anwendungen entwickelt, sind mehr Regelungen erforderlich, als wenn ein Unternehmen lediglich am Markt verfügbare Anwendungen einsetzt.

Die Richtlinie (»Policy«) sollte insbesondere Regelungen zu folgenden Punkten enthalten

- Anwendungsbereich, Definitionen
- Nennung, welche KI von welchem Anbieter zu welchem Zweck in welchem Unternehmensbereich zur Nutzung erlaubt ist
- Gestattung oder Verbot der Privatnutzung
- KI-Prinzipien oder Leitbild des Unternehmens bzgl. der Entwicklung und Nutzung von KI
- Grundsätze der Nutzung
- Dokumentations-, Kennzeichnungs- und Transparenzanforderungen
- Zuständigkeiten, Genehmigungserfordernisse, Aufklärungs- und Sanktionsmechanismen bei Missachtung der Richtlinien
- Bezüge zu anderen internen Richtlinien und zu externen regulatorischen Vorgaben
- Verweis auf weitere Regelungen

Die weiteren Regelungen (z. B. »Standards«) können beliebige weitere Felder abdecken. Beispiele sind

- Details der Dokumentation von KI-Systemen und Modellen
- Verfahren zur Sicherstellung von Fairness, Transparenz und Interpretierbarkeit, Zuverlässigkeit, Vermeidung von Voreingenommenheit (»bias«) Compliance und Regulierung: Sicherstellung der Einhaltung geltender Gesetze wie der KI-Verordnung und weiterer Regulierungen, Terms of Use und branchenspezifischer Standards im Kontext der Entwicklung/Nutzung von KI-Systemen und Modellen
- Vorgaben für die Beschaffung/den Einkauf von Anwendungen mit KI-Komponenten
- Handlungsanforderungen/-empfehlungen für die Angestellten
- Einzelheiten des Risikomanagementsystems und des Qualitätsmanagementsystems IP Recht (u. a. urheberrechtliche Aspekte bei Nutzung von Daten zu Training/Entwicklung/Adaptierung von KI-Modellen und Systemen)
- Überwachung von Modellen im Einsatz, die mit hohem Risiko behaftet sind
- Nutzung von personenbezogenen und nicht personenbezogenen Daten für die Entwicklung, das Testen und den Einsatz von Modellen
- Sicherheit und Informationssicherheit von KI-Anwendungen
- Regelungen für einzelne Anwendungsfelder (»Use Cases«) – etwa KI-Einsatz im Bewerbungsverfahren, in der Personaladministration
- Verhältnis zu benachbarten Themenfeldern, z. B. Datenschutz, Geschäfts-geheimnisschutz, Urheberrecht
- evtl. ergänzende oder abweichende Regeln für unterschiedliche Länder.

Dabei sollte auch berücksichtigt werden, dass die Mitarbeiter in geeigneter Weise geschult werden, um die jeweils relevanten Regelungen kennen und anwenden zu können.

Training eigener KI

Sofern man den Einsatz von KI-Techniken in seinem Unternehmen etablieren möchte, kann auch die Entwicklung eines eigenen KI-Systems oder Modells in Betracht gezogen werden. Damit ein solches System oder Modell jedoch effektiv arbeitet und letztlich positive Effekte erzielt werden können, muss es intensiv trainiert werden. Dieser Leitfaden verzichtet an dieser Stelle auf detaillierte Ausführungen, da die bisherigen Erfahrungen mit dem Training eigener KI noch nicht hinreichend ausgereift sind, aber auch die letztendliche Relevanz des Einsatzes eigener KI noch unbekannt ist. Ein Blick in die Praxis zeigt, dass bislang vor allem die Nutzung bereits etablierter KI-Modelle im Vordergrund steht und die Vielzahl unternehmenseigener KI-Systeme nicht über die Entwicklungsphase hinaus besteht.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in
Isabelle Stroot | Referentin Datenschutz
T 030 27576-228 | i.stroot@bitkom.org

Verantwortliches Bitkom-Gremium
AK Datenschutz

Titelbild
© Irina Vodneva – istockphoto.com.