Kompass Inklusiv.

Datenschutz und Künstliche Intelligenz

Informationsblatt

Web: www.ki-kompass-inklusiv.de
E-Mail: info@ki-kompass-inklusiv.de

Initiiert durch:

dfki Deutsches Forschungszentrum für Künstliche Intelligenz German Research Center for Artificial Intelligence

BAG BBW Bundesarbeitsgemeinschaft BERUFSBILDUNGSWERKE

Deutsche Berufsförderungswerke Bundesverband

BAG WfbM Bundesarbeitsgemeinschaft Werkstätten für behinderte Menschen e.V.

Gefördert durch:

Bundesministerium für Arbeit und Soziales

aus Mitteln des Ausgleichsfonds

Kompass Inklusiv.

Das Informationsblatt wurde im November 2025 erstellt. Die gesetzlichen Grundlagen zum Datenschutz können sich weiterentwickeln. Für eine umfassende und aktuelle (datenschutz-)rechtliche Beurteilung zum Einsatz von KI-gestützten Assistenzsystemen im Arbeitskontext wird die Zusammenarbeit mit Fachanwält*innen empfohlen.

Zur besseren Lesbarkeit wird in diesem Infoblatt bei Auszügen aus Gesetzestexten das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

In der Datenschutz-Grundverordnung wird grundsätzlich keine gendersensible Sprache verwendet. Zur eindeutigen Zuordnung definierter Begriffe wie ‚Verantwortlicher', ‚Empfänger' oder `Vertreter' verzichten wir in diesem Informationsblatt ebenfalls auf eine Unterscheidung zwischen Geschlechtern.

Kompass Inklusiv.

Inhalt

Einführung 4

Was ist Datenschutz? 4

Was sind personenbezogene Daten? 5

Welche Gesetze und Regelungen schützen personenbezogene Daten? 6

Grundlegende Regelungen der Datenschutz-Grundverordnung 7

- Begriffserklärungen 7
- Zweckbindung 7
- Rechtsgrundlage 8
- Besondere Kategorien personenbezogener Daten 9
- Transparenzpflichten 11

Was sind Gesundheitsdaten? 11

Kann Künstliche Intelligenz datenschutzkonform eingesetzt werden? 12

Was ist eine Datenschutzerklärung? 15

Welche Maßnahmen zum Schutz personenbezogener Daten gibt es? 16

Wie ist die Haftung bei Verstößen gegen die DSGVO geregelt? 18

Literaturverzeichnis 19

Einführung

Dieses Informationsblatt richtet sich insbesondere an Nutzer*innen von KI-gestützten Assistenzsystemen. Es beleuchtet einige grundlegende Aspekte zum Schutz personenbezogener Daten beim Einsatz von Künstlicher Intelligenz am Arbeitsplatz von Menschen mit Behinderungen. Ein besonderes Augenmerk liegt dabei auf dem Schutz von Gesundheitsdaten, weil solche Daten mitunter erhoben und verarbeitet werden, wenn Menschen mit Behinderungen digitale oder KI-gestützte Technologien für eine bessere Teilhabe am Arbeitsleben nutzen.

Was ist Datenschutz?

Datenschutz bezeichnet den Schutz personenbezogener Daten, welche durch verantwortliche Stellen (siehe Kapitel Begriffserklärung) verarbeitet werden. Ziel ist dabei der Schutz der Privatsphäre und der Persönlichkeitsrechte der betroffenen Menschen. Eine ‚betroffene Person' ist eine natürliche Person, deren personenbezogene Daten verarbeitet werden. Digitale oder auch KI-Technologien nutzen oftmals personenbezogene Daten, um individuell und bedarfsgerecht zu (re)agieren. Je nach Technologie werden personenbezogene Daten beispielsweise auch über Sensoren, Kameras und Mikrofone erhoben. Mit Hilfe von KI-gestützten Systemen können sie besonders umfangreich analysiert und ausgewertet werden. In diesem Zusammenhang entstehen einige Fragen:

- Welche Daten werden erhoben?
- Wo und wie werden diese Daten gespeichert?
- Wer kann auf die Daten zugreifen?
- Wie und wofür werden die Daten ausgewertet?
- Wie kann ich sicherstellen, dass meine Daten nicht zweckentfremdet werden?
- Wie können Anwender*innen bestimmen, was mit ihren Daten passiert?

Quelle: (KI.ASSIST, 2022)

Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, mit denen eine Person eindeutig identifiziert werden kann. Im Alltag wird regelmäßig auf die Erfassung von personenbezogenen Daten aufmerksam gemacht, wenn Verträge, Einverständniserklärungen oder Nutzungsbestimmungen unterschrieben oder bestätigt werden müssen. Die Erfassung der Daten kann unter anderem zur Personalisierung von IT-Produkten, zu Abrechnungszwecken, für andere administrative Zwecke (z.B. Kundendienst) oder zu Werbezwecken erfolgen. Der Begriff „personenbezogene Daten" wird in Art. 4 Abs. 1 DSGVO definiert.

In der Praxis sind personenbezogene Daten zum Beispiel:

- Name und Vorname
- Anschrift
- E-Mail-Adresse
- Telefonnummer
- Geburtsdatum
- Sozialversicherungsnummer
- IP-Adresse, wenn sie einer bestimmten Person zugeordnet werden kann
- Standortdaten, die das Bewegungsprofil einer Person abbilden können
- Bilder und Videos, auf denen Personen erkennbar sind
- Biometrische Daten (z.B. Fingerabdrücke, Gesichtserkennung, Stimmerkennung)
- Gesundheitsdaten (siehe auch Abschnitt Gesundheitsdaten)
- Ethnische Zugehörigkeit
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit

Die genaue Auslegung und der Umfang des Begriffs „personenbezogene Daten" muss in Einzelfällen immer wieder auch gerichtlich geklärt werden. Beispielsweise hat das Landesgericht Kassel in einem Fall geurteilt, dass ein Fahrzeugkennzeichen im konkreten Einzelfall nicht als personenbezogenes Datum zu betrachten ist (Landesgericht Kassel 1, 2007). Das Verwaltungsgericht Schwerin hat sich mit Fotos eines Wohnhauses beschäftigt und in diesem konkreten Fall geurteilt, dass es sich bei den Fotos durchaus um

personenbezogene Daten handelt (Verwaltungsgericht Schwerin, 2021). In anderen Fällen kamen Gerichte in Bezug auf Fahrzeugkennzeichen und Fotos von Wohnhäusern zu anderen Ergebnissen. Daher muss bei der Datenerfassung immer umfassend und individuell geprüft werden, ob im vorliegenden Kontext personenbezogene Informationen erhoben werden.

Welche Gesetze und Regelungen schützen personenbezogene Daten?

Die Mindeststandards zum Schutz personenbezogener Daten sind für alle Länder der Europäischen Union in der Datenschutz-Grundverordnung (DSGVO) festgelegt. In diesem Gesetz ist geregelt, ob und wie personenbezogene Daten verarbeitet werden dürfen. Der Schutz natürlicher Personen wird in diesem Gesetz technologieunabhängig betrachtet.

Die europäische DSGVO bietet Raum für spezifische Anpassungen und Regelungen auf nationaler Ebene (Art. 6 Abs. 2 und 3 DSGVO, Art. 88 DSGVO). Das Bundesdatenschutzgesetz (BDSG) sowie die Landesdatenschutzgesetze (LDSG) der deutschen Bundesländer ergänzen und konkretisieren die DSGVO in Deutschland. Gesetzliche Datenschutzbestimmungen sind branchen- und berufsbezogen in weiteren nationalen Gesetzen verankert, weshalb diese zusätzlich zu berücksichtigen sind.

Das Bundesdatenschutzgesetz enthält zum Beispiel besondere Vorgaben und Sicherheitsmaßnahmen für den Umgang mit Gesundheitsdaten, welche über die Regelungen der DSGVO hinausgehen. Dies betrifft unter anderem die Verarbeitung dieser Daten für Forschungszwecke (§27 BDSG) oder für automatisierte Entscheidungen in der Versicherungswirtschaft, z.B. durch Krankenversicherungen (§37(2) BDSG). In Deutschland gibt es zusätzlich nationale Regelungen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen oder Arbeitgeber oder auch für statistische Zwecke.

Grundlegende Regelungen der Datenschutz-Grundverordnung

Einige Vorgaben der DSGVO sind in Bezug auf den Einsatz von KI-gestützten Assistenzsystemen für Menschen mit Behinderungen am Arbeitsplatz besonders erwähnenswert. Diese werden im Folgenden kurz erläutert.

Begriffserklärungen

Art. 4 DSGVO definiert grundlegende Begriffe der DSGVO. Im Artikel 4 werden unter anderem die Begriffe ‚Verantwortlicher' und ‚personenbezogene Daten' sowie auch ‚Verarbeitung' erklärt.

Der Verantwortliche ist eine Person oder Organisation, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Sie ist dafür verantwortlich, dass die Datenverarbeitung den Vorschriften der DSGVO entspricht. Die Anwender*innen eines Computerprogramms können unter Umständen ebenso wie dessen Anbieter Verantwortliche für die Erfassung und Verarbeitung von Daten sein, wenn sie bei der Nutzung des Computerprogramms personenbezogene Daten von betroffenen Personen verarbeiten.

‚Verarbeitung' meint „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung."

Zweckbindung

Art. 5 DSGVO regelt unter Abs. 1 lit. b), dass jede Datenerhebung einer Zweckbindung unterliegen muss. Der oder die Verantwortliche der Datenverarbeitung muss den Zweck der Datenverarbeitung eindeutig definieren und darf die erhobenen Daten nach der Erhebung nicht für andere Zwecke verwenden.

Rechtsgrundlage

Art. 6 DSGVO bestimmt in Absatz 1, dass die Verarbeitung personenbezogener Daten nur unter bestimmten Bedingungen stattfinden darf. Das bedeutet, dass Verantwortliche je nach Zweck der Datenverarbeitung diese Verarbeitung entsprechend einer von sechs Bedingungen von Art. 6 Abs. 1 lit. a) bis f) DSGVO unterwerfen müssen. Es handelt sich um die Rechtsgrundlage, auf welcher eine Datenverarbeitung stattfindet. Dies kann eine Einwilligung oder die Vertragsanbahnung bzw. Vertragserfüllung sein (Art. 6 Abs. 1 lit a) und b) DSGVO).

Die Interessensabwägung (Art. 6 Abs. 1 lit f) DSGVO) ist als Rechtsgrundlage für die Datenerfassung durch Assistenzsysteme ebenfalls hervorzuheben. Bei dieser Bedingung ist die Zustimmung der Betroffenen nicht notwendig, jedoch haben Betroffene immer ein Widerspruchsrecht (Art. 21 DSGVO) gegenüber der verantwortlichen Stelle. Die Verarbeitung von personenbezogenen Daten darf gemäß dieser Rechtsgrundlage nur dann erfolgen, wenn diese „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt." (Art. 6 Abs. 1 lit. f) DSGVO). Die Beurteilung, ob und wie schwer die Grundrechte und Grundfreiheiten der betroffenen Personen die Interessen der verantwortlichen Stelle überwiegen, muss mehrstufig vor Beginn der Datenverarbeitung bei der verantwortlichen Stelle erfolgen.

Die Rechtsgrundlage ergibt sich immer aus dem Zweck der Verarbeitung und hängt immer mit den Umständen der Erforderlichkeit der Datenverarbeitung zusammen. Das bedeutet, dass die Rechtsgrundlage für die verantwortliche Stelle nicht frei wählbar oder frei bestimmbar ist, sondern hergestellt werden muss.

In einer der Rechtsexpertisen zum Forschungsprojekt KI.ASSIST (Borges, 2022) wird am Beispiel von Datenbrillen zur videobasierten und automatisierten Identifizierung von Personen dargestellt, dass die Verarbeitung personenbezogener Daten (z.B. Videoaufnahmen von fremden Personen) zum Ausgleich einer Schwerbehinderung unter Umständen als berechtigtes Interesse mit Verweis auf Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt werden kann.

Die Rechtsexpertise geht dabei darauf ein, dass auch technische Spezifikationen von Technologien (z.B. Ort der Datenverarbeitung, Anbindung an externe Datenbanken oder auch die Begrenzungen der Speicherkapazität) bei der juristischen Beurteilung der Rechtmäßigkeit der Datenverarbeitung entsprechend Art. 6 Abs. 1 lit. f DSGVO eine wichtige Rolle spielen können.

Besondere Kategorien personenbezogener Daten

Art. 9 DSGVO definiert besondere Kategorien personenbezogener Daten. Diese Kategorien behandeln besonders sensible Daten, welche durch die DSGVO zusätzlich geschützt werden.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist untersagt. Es gibt jedoch nach Art. 9 Abs. 2 lit. a) bis j) DSGVO zehn Ausnahmeregelungen, unter welchen die Verarbeitung solcher Daten rechtmäßig ist.

Zu den Daten der besonderen Kategorie personenbezogener Daten gehören:

- Gesundheitsdaten (siehe auch Abschnitt Gesundheitsdaten)
- biometrische Daten
- genetische Daten
- Gewerkschaftszugehörigkeit
- Daten zu rassischer und ethnischer Herkunft
- religiöse und weltanschauliche Überzeugungen
- politische Meinungen
- Daten zum Sexualleben oder zur sexuellen Orientierung

Die Zustimmung der Betroffenen ist wie in Art. 6 DSGVO eine Möglichkeit, um diese sensiblen Daten verarbeiten zu können. In Verbindung mit den Regelungen in Art. 6 DSGVO muss der Verantwortliche die Ausnahmeregelungen zusätzlich berücksichtigen.

Beispiel zur Verarbeitung von Gesundheitsdaten ohne Zustimmung der Betroffenen:

Der Betriebsrat eines Unternehmens kann vom Arbeitgeber auch ohne Zustimmung der Betroffenen eine Liste aller Mitarbeiter*innen mit Schwerbehinderungen oder gleichgestellten Personen verlangen. In diesem Fall liegt eine Verarbeitung von Gesundheitsdaten vor. Entsprechend § 80 Abs. 2 S. 1 BetrVG steht dem Betriebsrat zu, dass er über alle relevanten Informationen verfügt, welche er benötigt, um seinen Aufgaben nachzukommen. Unter diese Aufgaben fällt laut § 80 Abs. 1 Nr. 4 BetrVG auch die Förderung der Eingliederung von Menschen mit Schwerbehinderungen. Art. 9 Abs. 2 lit. b DSGVO rechtfertigt die Verarbeitung von Gesundheitsdaten der Arbeitnehmer*innen, wenn diese im Zusammenhang mit Rechten aus dem Arbeitsrecht, der sozialen Sicherheit oder des Sozialschutzes steht. Zu diesem konkreten Fall hat das Bundesarbeitsgericht im Jahr 2023 geurteilt (Bundesarbeitsgericht, 2023).

Die dargestellte Regelung kann hilfreich sein, wenn ein Betriebsrat zur Erstellung einer Betriebsvereinbarung für den Einsatz von Künstlicher Intelligenz in Unternehmen auch die Interessen von Menschen mit Schwerbehinderungen erheben und angemessen berücksichtigen möchte.

Transparenzpflichten

Die Artikel 12 bis 14 der DSGVO geben vor, in welchem Umfang die oder der Betroffene über die Verarbeitung personenbezogener Daten informiert werden muss (siehe Kapitel Datenschutzerklärung). Die Informationen müssen durch den Verantwortlichen verständlich formuliert und leicht zugänglich sein. Zunehmend werden Datenschutzerklärungen auf Webseiten auch in Leichter Sprache veröffentlicht. Diese vereinfachten Datenschutzerklärungen sind in der Regel jedoch nicht rechtsverbindlich. Art. 12 Abs. 7 DSGVO regelt, dass die Informationen in Datenschutzerklärungen „in Kombination mit standardisierten Bildsymbolen bereitgestellt werden können, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein." Diese Regelung kann für die Barrierefreiheit von Datenschutzerklärungen hilfreich sein.

Was sind Gesundheitsdaten?

Gesundheitsdaten gehören zu den besonderen Kategorien personenbezogener Daten. Gemäß Artikel 4 der DSGVO werden Gesundheitsdaten definiert als „personenbezogene Daten, die sich auf die physische oder psychische Gesundheit einer natürlichen Person beziehen, einschließlich der Erbringung von Gesundheitsdienstleistungen, aus denen sich Informationen über ihren Gesundheitszustand ergeben."

Zu den Gesundheitsdaten gehören unter anderem:

- Medizinische Diagnosen
- Informationen über Behandlungen und medizinische Eingriffe
- Ergebnisse von medizinischen Untersuchungen und Tests
- Informationen über Medikationen
- Genetische Daten (beispielsweise Daten, die aus der Analyse von biologischen Proben gewonnen werden)
- Daten über psychische Gesundheit (z.B. auch Emotionsanalysen)
- Informationen aus der Gesundheitsüberwachung (z.B. auch von Fitness-Trackern, Smartwatches etc.)

Gesundheitsdaten werden insbesondere im medizinischen Bereich (z.B. in der digitalen Patientenakte) verarbeitet. Durch die zunehmende Verbreitung von

Fitness-Trackern, Smartwatches oder digitalen Gesundheitsanwendungen werden Gesundheitsdaten jedoch verstärkt auch in anderen Lebensbereichen verarbeitet.

Auch beim Einsatz von digitalen und KI-gestützten Assistenzsystemen an Arbeitsplätzen kann eine regelmäßige Verarbeitung von Gesundheitsdaten stattfinden.

> In den Lern- und Experimentierräumen des Forschungsprojekts KI.ASSIST wurden die Technologien EmmA, EmpaT, OPTAPEB und AirCrumb als Systeme mit therapeutischem Hintergrund in der Ausbildung erprobt (Thieke-Beneke, et al., 2022). Die verarbeiteten Daten dieser Systeme (u.a. Atemfrequenz, Stimmlage oder auch Augenbewegungen) lassen unter bestimmten Umständen Rückschlüsse auf den Gesundheitszustand der Nutzer*innen zu. Die Datensammlung in den genannten Lern- und Experimentierräumen wurden zur Bewertung oder Verbesserung der Gesundheit und des Wohlbefindens der Betroffenen verwendet, sodass es sich bei diesen Daten um Gesundheitsdaten handelt.

Kann Künstliche Intelligenz datenschutzkonform eingesetzt werden?

Die Nutzung von Künstlicher Intelligenz bringt neue Aspekte zum Datenschutz mit sich. KI-Modelle benötigen oft große Datenmengen, um die gewünschten Funktionen eines KI-Systems trainieren und ausführen zu können. Sowohl in der Trainingsphase als auch bei der anschließenden Anwendungsphase (Nutzung) von KI-Systemen ist die Verarbeitung von Daten essenziell. Dies kann auch die Verarbeitung persönlicher Daten beinhalten.

Stimmanalysen, Gesichtserkennung, Fingerabdruckerkennung, Puls-, Sauerstoff- und Blutdruckmessungen halten immer häufiger Einzug in digitale Produkte. Der Schutz personenbezogener Daten wird mit der zunehmenden Verbreitung von KI somit immer wichtiger und anspruchsvoller.

Ein System zur Spracherkennung kann zum Beispiel mit einer großen Menge von Sprachaufnahmen trainiert werden. Hierbei wird darauf geachtet, dass ein möglichst breites Spektrum an Daten, zum Beispiel auch unter Berücksichtigung von Akzenten und regionalen Dialekten, für das Training eines Spracherkennungsmodells genutzt wird. Diese Form personenbezogener Daten ist notwendig und zweckdienlich, damit ein Spracherkennungsmodell funktioniert. Bei der anschließenden Nutzung eines Sprachmodells müssen ebenso Sprachaufnahmen der Betroffenen verarbeitet werden. (Flock & Spieker, 2015)

Verschiedene Aspekte der Datenverarbeitung für KI-Modelle stehen heute in Konflikt mit der DSGVO.

Die notwendigen Datenmengen für die Entwicklung und Nutzung von KI-Systemen sind beispielsweise häufig eine Herausforderung für das Prinzip der Datenminimierung entsprechend Art. 5 Abs. 1 lit. c DSGVO. Entwickler von KI-Modellen haben jedoch selbst aus wirtschaftlichen Gründen, zur Qualitätsoptimierung und zur Steigerung der Verarbeitungsgeschwindigkeit von KI-Modellen in einigen Fällen ein eigenes Interesse an Datenminimierung. Diese Entwicklung ist zurzeit beispielsweise bei kleinen KI-Modellen für den lokalen Betrieb auf Endgeräten zu beobachten.

Wissenschaftliche Studien belegen, dass größere KI-Modelle und mehr Trainingsdaten bei der Anwendung nicht proportional zu besseren Ergebnissen führen (Emma Strubell, 2019). Ab einer bestimmten Menge an Trainingsdaten wird bei KI-Modellen ein Sättigungspunkt erreicht, bei welchem Verbesserungen nur durch einen unverhältnismäßig größeren Berechnungs- und Energieaufwand erreicht werden können. Durch Datenminimierung und eine qualitätsorientierte Auswahl von Trainingsdaten kann neben der DSGVO-Konformität daher auch der Energieverbrauch von KI-Modellen beim Training und bei der Anwendung der Modelle positiv beeinflusst werden.

Die Effizienz von KI-Modellen, auch in Hinblick auf Energieverbrauch und Verarbeitungszeit für eine Rechenoperation, wird als wichtiger Faktor für die Wettbewerbsfähigkeit zukünftiger KI-Modelle betrachtet (Gundlach, Lynch, Mertens, & Thompson, 2025).

Die Algorithmen von KI-Modellen, welche auf künstlichen neuronalen Netzen basieren, sind komplex und die daraus entstehenden Berechnungen sind nicht eindeutig erklärbar (Deutscher Ethikrat, 2023). Die Datenverarbeitung und Entscheidungsfindung von KI-Systemen sind daher sowohl für die betroffenen Personen als auch für die Verantwortlichen nicht vollumfänglich nachvollziehbar. Betroffene müssen jedoch gemäß den Artikeln 12 bis 14 DSGVO transparent darüber informiert werden, wie ihre Daten verarbeitet und ob automatisierte Entscheidungen getroffen werden. Die Bereitstellung einer transparenten Information zum Umfang der Datenverarbeitung erscheint damit nur bedingt möglich.

Betroffene haben zudem entsprechend den Artikeln 15, 16, 17, 21 DSGVO beispielsweise das Recht auf Auskunft, Berichtigung und Löschung sowie auf Widerspruch zur Verarbeitung ihrer Daten. Die Umsetzung dieser Rechte kann bei KI-Systemen kompliziert sein. Schwierigkeiten treten insbesondere auf, wenn Betroffene eine Berichtigung oder Löschung von Daten in KI-Modellen wünschen, da die KI-Modelle hierfür unter Umständen mit hohem Aufwand neu trainiert werden müssen (Holzki, 2023).

Die Optimierung von KI-Modellen und Änderungen an Trainingsdaten erfordern eine fortlaufende Neubewertung und Anpassung der Datenschutzmaßnahmen. Aufgrund von gewollt zufälliger Prozesse bei der Datenverarbeitung kann es vorkommen, dass KI-Modelle bei wiederholter Ausführung und identischer Dateneingaben unterschiedliche Ergebnisse liefern. Dieser Effekt ist häufig gewünscht, damit z.B. generative KI-Modelle eine Vielzahl von Ergebnissen auf eine identische Eingabe liefern können. Aufgrund dieser Voraussetzung können die Verantwortlichen häufig jedoch nicht abschließend beurteilen, ob die getroffenen Maßnahmen zum Datenschutz bei der Erstellung und Verbreitung eines KI-Modells ausreichend sind.

Der Ort, an dem Daten verarbeitet werden, spielt eine besonders wichtige Rolle in Bezug auf Künstliche Intelligenz. Daten können entweder lokal auf einem Gerät oder in einem sicheren Rechenzentrum verarbeitet werden. Durch eine lokale Datenverarbeitung behalten die Betroffenen die volle Kontrolle über ihre Daten. Datenlecks, Hackerangriffe und Missbrauch von personenbezogenen Daten durch Drittanbieter werden erschwert, wenn die sensiblen Daten das Gerät nicht verlassen. Das setzt jedoch voraus, dass die Betroffenen vollumfängliche Fachexpertise und Mittel zur Sicherung ihrer lokalen Daten selbst bereitstellen und einbringen. Die Verarbeitung von KI-Modellen erfordert außerdem häufig sehr leistungsfähige Computer, sodass eine lokale Datenverarbeitung nicht immer möglich ist.

Kompass Inklusiv.

Was ist eine Datenschutzerklärung?

Die Datenschutzerklärung soll betroffene Personen über die Verarbeitung personenbezogener Daten informieren. Die Bereitstellung einer Datenschutzerklärung ist für die Verantwortlichen der Datenverarbeitung verpflichtend.

Art. 13 und 14 DSGVO regeln die Informationspflichten der Verantwortlichen gegenüber den Betroffenen. Inhaltlich umfasst dies folgende Punkte:

1. Kontaktdaten des Verantwortlichen für die Datenverarbeitung.
2. Zwecke der Datenverarbeitung: Dies umfasst sowohl die Hauptzwecke der Datenverarbeitung als auch eventuelle Nebenverwendungen der Daten (z.B. Marketing).
3. Rechtsgrundlage der Verarbeitung: Es muss angegeben werden, auf welcher rechtlichen Grundlage die Datenverarbeitung erfolgt.
4. Empfänger der Daten: Die Betroffenen müssen informiert werden, ob ihre personenbezogenen Daten an Dritte weitergegeben werden und wer diese Empfänger sind (z.B. Dienstleister, Partnerunternehmen).
5. Übermittlung in Drittländer: Wenn personenbezogene Daten in Länder außerhalb der Europäischen Union (Drittländer) übermittelt werden, muss dies angegeben werden. Zudem müssen Informationen bereitgestellt werden, welche Garantien bestehen, um die Datenübermittlung zu rechtfertigen.
6. Dauer der Datenspeicherung: Die Betroffenen müssen darüber informiert werden, wie lange ihre personenbezogenen Daten gespeichert werden.
7. Rechte der Betroffenen:

   Die Betroffenen müssen über ihre Rechte informiert werden. Dazu gehören:

   - Recht auf Auskunft über die verarbeiteten Daten
   - Recht auf Berichtigung unrichtiger Daten
   - Recht auf Löschung
   - Recht auf Datenübertragbarkeit
   - Widerspruchsrecht gegen die Verarbeitung
   - Widerruf der Einwilligung: Die Betroffenen müssen darüber informiert werden, dass sie ihre Einwilligung jederzeit widerrufen können.

8. Beschwerderecht bei einer Aufsichtsbehörde:

   Die Betroffenen müssen darüber informiert werden, dass sie das Recht haben, eine Beschwerde bei einer Aufsichtsbehörde einzureichen, wenn sie der Meinung sind, dass die Verarbeitung ihrer personenbezogenen Daten gegen die DSGVO verstößt.

9. Informationen zu einer automatisierten Entscheidungsfindung oder einem Profiling.

Welche Maßnahmen zum Schutz personenbezogener Daten gibt es?

Betroffene Personen können selbst verschiedene Maßnahmen ergreifen, um ihre personenbezogenen Daten zu schützen.

Sie sollten zunächst immer die Datenschutzerklärung aufmerksam lesen und inhaltlich erfassen, bevor sie ihre Daten in einer Anwendung oder auf einer Plattform preisgeben. Dies ist eine wichtige Voraussetzung, um eine informierte Entscheidung treffen zu können. Darüber hinaus sollten sie sich informieren, wie sie die Datenschutzeinstellungen bei der Nutzung von Computerprogrammen nach ihren Bedürfnissen anpassen können. Dazu gehören Einstellungen zur Kontrolle, welche Daten erfasst werden, wo sie gespeichert werden und wer darauf zugreifen kann. Arbeitgeber können ihre Mitarbeiter*innen beim Schutz personenbezogener Daten unterstützen, indem sie Schulungen anbieten und damit das Bewusstsein für Datenschutz und Datensicherheit beim Umgang mit der Unternehmens-IT schärfen. All diese Maßnahmen tragen wesentlich zur Datensouveränität der Betroffenen bei (Kähler, 2022).

Wie oben beschrieben, sind die Verantwortlichen der Datenverarbeitung aufgrund der DSGVO zu umfangreichen Maßnahmen für den Datenschutz gesetzlich verpflichtet. Sie müssen alle Maßnahmen ergreifen, welche die Vertraulichkeit von Daten hinsichtlich Datenschutz und Datensicherheit gewährleisten (Art. 5 Abs. 1 lit. f) DSGVO).

Das Prinzip der Datensparsamkeit besagt, dass nur die für den jeweiligen Zweck notwendige Daten erhoben und verarbeitet werden dürfen. Es ist unzulässig, Daten zu erheben, die nicht für den jeweiligen Zweck der Verarbeitung erforderlich sind. Wie im Kapitel „Kann Künstliche Intelligenz datenschutzkonform eingesetzt werden?“ beschrieben, ist das Prinzip der Datenminimierung bei der Entwicklung und beim Einsatz KI-gestützter Systeme jedoch häufig eine Herausforderung.

Durch Anonymisierung möchten die Verantwortlichen personenbezogene Daten so verändern, dass die Daten nachträglich nicht mehr einer bestimmten Person zugeordnet werden können. Pseudonymisierung bedeutet hingegen, dass identifizierende Merkmale durch ein Pseudonym ersetzt werden, sodass eine Rückverfolgung nachträglich noch mit zusätzlichen Informationen (z.B. eine sicher verwahrte Liste mit der Zuordnung von Pseudonym und Originaldaten) möglich ist. Beide Methoden reduzieren das Risiko, dass personenbezogene Daten einen Rückschluss auf eine natürliche Person ermöglichen. (Weiß & Alsabah, 2020).

Ein recht neuer Ansatz für den Datenschutz ist das Training von KI-Modellen mit Hilfe von synthetischen Daten. Hierbei wird ein Datensatz mit echten Daten verwendet, um daraus neue, künstliche Daten mit ähnlichen statistischen Eigenschaften zu erstellen. KI-Modelle sollen sich mit solchen Daten datenschutzfreundlich trainieren lassen. Der unberechtigte Zugriff von Dritten auf synthetische Daten ist darüber hinaus datenschutzrechtlich unbedenklich (Kompetenzzentrum Öffentliche IT, 2023).

Zur Anonymisierung und Pseudonymisierung von Daten sowie zur Erstellung synthetischer Daten können heute ebenfalls KI-Modelle eingesetzt werden.

Bei der Verschlüsselung von Daten werden diese in eine nicht lesbare Form umgewandelt, die nur durch Verwendung eines speziellen Schlüssels wiederhergestellt werden kann. Diese Methode kann Daten sowohl bei der Übertragung (z.B. im Internet) als auch bei der Speicherung vor unbefugtem Zugriff schützen.

Technische Vorkehrungen wie die lokale Verarbeitung von KI-Modellen (sogenannte Edge AI) und spezialisierte Computerchips (z.B. Neural Processing Units) können dabei helfen, den Datenschutz im Sinne der Betroffenen zu erhöhen. Die lokale Verarbeitung von Daten bedeutet, dass alle Daten, die für die Ausführung eines KI-Modells benötigt werden, direkt auf dem Gerät der Nutzer*innen verarbeitet werden, anstatt sie an externe Server zu senden. Dies reduziert das Risiko, dass sensible Daten während der Übertragung abgefangen oder auf unsicheren Servern gespeichert werden (Ecker, 2024).

Unabhängig vom Speicherort der Daten sollte der Zugriff auf personenbezogene Daten streng kontrolliert und dokumentiert werden. Nur autorisierte Personen sollten Zugang zu den Daten haben, und es sollte nachvollziehbar sein, wer wann auf welche Daten zugegriffen hat.

Bekannte Beispiele für die lokale Verarbeitung:

Spracherkennung: Sprachassistenten wie Siri oder Google Assistant können Sprachbefehle teilweise direkt auf dem Gerät verarbeiten, ohne dass Audiodaten an externe Server gesendet werden müssen. Dies schützt die Privatsphäre der Nutzer*innen und erhöht zudem die Geschwindigkeit der Datenverarbeitung.

Gesichtserkennung: Sicherheitsfunktionen wie die Gesichtserkennung zum Entsperren von Smartphones können lokal auf dem Gerät ausgeführt werden. Die Gesichtsdaten bleiben dabei sicher auf dem Gerät und werden nicht an externe Server übertragen.

Bilderkennung: Das Assistenzsystem OrCam MyEye2 kann mit Hilfe einer Kamera und nach einer kurzen Trainingsphase die Gesichter von bis zu 100 Personen eindeutig identifizieren (Borges, 2022). Die Datenverarbeitung findet dabei ausschließlich lokal auf dem Gerät statt und schützt damit personenbezogene Daten.

Wie ist die Haftung bei Verstößen gegen die DSGVO geregelt?

Die DSGVO legt in den Art. 82, 83, 58 und 59 umfassende Haftungsregelungen fest, um den Schutz personenbezogener Daten zu gewährleisten und Verantwortliche sowie Auftragsverarbeiter zur Rechenschaft zu ziehen. Diese Regelungen umfassen die Schadenersatzpflicht, die solidarische Haftung, Entlastungsmöglichkeiten, erhebliche Bußgelder und die Befugnisse der Aufsichtsbehörden, Sanktionen zu verhängen.

Die Einhaltung der DSGVO wird in Deutschland von verschiedenen staatlichen Stellen kontrolliert und durchgesetzt. Dazu gehören die Datenschutzaufsichtsbehörden der Länder und die Bundesbeauftragte für den Datenschutz. Betroffene haben das Recht, bei ihrer Datenschutzbehörde Beschwerden einzureichen, wenn sie der Ansicht sind, dass ihre Rechte gemäß der DSGVO verletzt wurden. Unabhängig von der Beschwerde bei der Aufsichtsbehörde können Betroffene auch zivilrechtlich gegen Datenschutzverstöße bei einer verantwortlichen Stelle vorgehen und beispielsweise gerichtlich eine Klage mit Schadenersatzansprüchen einreichen.

Literaturverzeichnis

Borges, G. (2022). *Rechtsfragen von KI-Systemen in der beruflichen Rehabilitation für Menschen mit Schwerbehinderung. Datenschutz, Haftung und KI-Regulierung. Rechtliche Expertise im Projekt KI.ASSIST.* Bundesverband Deutscher Berufsförderungswerke e. V.

Bundesarbeitsgericht. (9. Mai 2023). *Beschluss vom 09.05.2023. Aktenzeichen 1 ABR 14/22.*

Deutscher Ethikrat. (2023). *Stellungnahme „Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz".*

Ecker, W. H. (2024). *Edge AI: KI nahe am Endgerät. Technologie für mehr Datenschutz, Energie effizienz und Anwendungen in Echtzeit.* München: Plattform Lernende Systeme. doi:https://doi.org/10.48669/pls_2024-4

Emma Strubell, A. G. (2019). *Energy and Policy Considerations for Deep Learning in NLP.* College of Information and Computer Sciences University of Massachusetts Amherst.

Flock, P., & Spieker, H. (2015). *Spracherkennung (Masterseminar).* Hochschule Bonn-Rhein-Sieg.

Gundlach, H., Lynch, J., Mertens, M., & Thompson, N. (2025). *The Price of Progress: Algorithmic Efficiency and the Falling Cost of AI Inference.* Von The Price of Progress: Algorithmic Efficiency and the Falling Cost of AI Inference: https://arxiv.org/abs/2511.23455 abgerufen

Holzki, L. (10. August 2023). *Warum es so schwierig ist, KI etwas abzutrainieren.* (handelsblatt.com, Herausgeber) Abgerufen am 12. 11 2024 von https://www.handelsblatt.com/technik/ki/kuenstliche-intelligenz-warum-es-so-schwierig-ist-ki-etwas-abzutrainieren/29314906.html

Kähler, M. (2022). *Datensouveränität, KI und Menschen mit Behinderungen. Konzepte, Analysen und Maßnahmen. Ergebnisbericht des Projekts KI.ASSIST.* Bundesverband Deutscher Berufsförderungswerke e. V.

KI.ASSIST. (2022). *Datenschutz und Datensouveränität*. Abgerufen am 12. 11 2024 von https://www.ki-assist.de/wissen/kuenstliche-intelligenz/datenschutz-und-datensouveraenitaet-2

Kompetenzzentrum Öffentliche IT. (25. Mai 2023). *Synthetische Daten – Künstliche Daten für die digitale Zukunft?* Abgerufen am 12. 11 2024 von https://www.oeffentliche-it.de/-/synthetische-daten

Landesgericht Kassel 1, 1 T 75/07 (LG Kassel 1. Beschwerdekammer 10. Mai 2007). Abgerufen am 12. 11 2024 von https://www.rv.hessenrecht.hessen.de/perma?d=LARE230004593

Thieke-Beneke, M., Stock, J., Biedermann, J., Stähler, L., Feichtenbeiner, R., & Lippa, B. (2022). *Die KI.ASSIST Lern- und Experimentierräume zur Erprobung KI-gestützter Assistenztechnologien. Von der Konzeption bis zur Umsetzung. Ergebnisbericht des Projekts KI.ASSIST.* Bundesverband Deutscher Berufsförderungswerke e. V.

Verwaltungsgericht Schwerin, 1 A 1343/19 SN (Verwaltungsgericht Schwerin 29. 04 2021). Abgerufen am 12. 11 2024 von https://landesrecht-mv.de/bsmv/document/NJRE001468715

Weiß, R., & Alsabah, N. (2020). *Einleitung zu „Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens*". AK Artificial Intelligence. Bitkom.