

Orientierungshilfe

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024

Künstliche Intelligenz und Datenschutz

Version 1.0

Viele Unternehmen, Behörden und andere Organisationen fragen sich derzeit, unter welchen Voraussetzungen sie KI-Anwendungen datenschutzkonform einsetzen können. Dabei lag der Schwerpunkt ab dem Jahr 2023 auf sogenannten Large Language Models (LLM), die häufig als Chatbots angeboten werden, aber auch als Grundlage für andere Anwendungen dienen können. Der Schwerpunkt der folgenden Orientierungshilfe liegt daher derzeit auf diesen KI-Anwendungen. Über die LLM hinaus gibt es jedoch zahlreiche weitere KI-Modelle und KI-Anwendungen, deren Einsatz infrage kommen kann und für die viele der folgenden Erwägungen ebenfalls relevant sein dürften.

Diese Orientierungshilfe bietet einen Überblick über datenschutzrechtliche Kriterien, die für die datenschutzkonforme Nutzung von KI-Anwendungen zu berücksichtigen sind. Sie kann als Leitfaden dienen, um KI-Anwendungen auszuwählen, zu implementieren und zu nutzen.

Die Orientierungshilfe wird voraussichtlich in der Zukunft angepasst werden, um aktuelle Entwicklungen und weitere relevante Aspekte aufzunehmen. Sie bietet einen Leitfaden, stellt aber keinen abschließenden Anforderungskatalog dar. Teilweise sind weitere Ressourcen hinzuzuziehen, um die in dieser Orientierungshilfe angesprochenen Punkte umzusetzen.

Die Orientierungshilfe richtet sich in erster Linie an die Verantwortlichen, die KI-Anwendungen einsetzen möchten. An Entwickler:innen, Hersteller:innen und Anbieter:innen von KI-Systemen richtet sie sich mittelbar, indem sie Hinweise zur Auswahl datenschutzkonformer KI-Anwendungen enthält. Die Entwicklung von KI-Anwendungen und das Training von KI-Modellen sind jedoch nicht Schwerpunkt dieser Orientierungshilfe.

Inhaltsverzeichnis

1.	Konzeption des Einsatzes und Auswahl von KI-Anwendungen	3
1.1	Einsatzfelder und Zwecke bestimmt?.....	3
1.2	Einsatzfelder rechtmäßig?.....	3
1.3	Einsatzfelder ohne personenbezogene Daten?	3
1.4	Datenschutzkonformes Training von KI-Anwendungen.....	4
1.5	Rechtsgrundlage für die Datenverarbeitung?.....	4
1.6	Keine automatisierte Letztentscheidung	5
1.7	Geschlossenes oder offenes System?.....	5
1.8	Transparenz.....	6
1.9	Transparenz und Wahlmöglichkeit hinsichtlich KI-Training	7
1.10	Transparenz und Wahlmöglichkeit hinsichtlich Eingabe-Historie	7
1.11	Berichtigung, Löschung und weitere Betroffenenrechte	7
1.12	Datenschutzbeauftragte und Beschäftigtenvertretung einbinden	8
2.	Implementierung von KI-Anwendungen	8
2.1	Verantwortlichkeit festlegen und verbindlich regeln	8
2.2	Interne Regelungen treffen	9
2.3	Datenschutz-Folgenabschätzung.....	10
2.4	Beschäftigte schützen, betriebliche Accounts einrichten	10
2.5	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.....	11
2.6	Datensicherheit	11
2.7	Beschäftigte sensibilisieren	12
2.8	Weitere Entwicklungen verfolgen	12
3.	Nutzung von KI-Anwendungen	12
3.1	Vorsicht bei Eingabe und Ausgabe personenbezogener Daten	12
3.2	Besondere Vorsicht bei besonderen Kategorien personenbezogener Daten.....	14
3.3	Ergebnisse auf Richtigkeit prüfen	14
3.4	Ergebnisse und Verfahren auf Diskriminierung prüfen.....	15

1. Konzeption des Einsatzes und Auswahl von KI-Anwendungen

1.1 Einsatzfelder und Zwecke bestimmt?

Vor dem Einsatz einer KI-Anwendung, sollten Verantwortliche explizit festlegen, welche Einsatzfelder für die KI-Anwendung vorgesehen sind und welchem Zweck diese konkret dient. Im Hinblick auf die Verarbeitung personenbezogener Daten ist diese Zweckfestlegung elementar für den datenschutzkonformen Betrieb, da nur aufgrund konkreter vorab festgelegter Zwecke überprüft werden kann, ob die Verarbeitung personenbezogener Daten zur Zweckerreichung erforderlich ist.

1

Für öffentliche Stellen ist es diesbezüglich auch wichtig, sicherzustellen, dass sich das Einsatzfeld im Rahmen der ihnen gesetzlich zugewiesenen öffentlichen Aufgaben befindet und eine Verarbeitung personenbezogener Daten in diesem Rahmen zur Aufgabenerfüllung erforderlich ist.

2

1.2 Einsatzfelder rechtmäßig?

Bestimmte Einsatzfelder für KI-Anwendungen können von vornherein unzulässig sein. So gelten nach der europäischen KI-Verordnung z. B. „Social Scoring“ und biometrische Echtzeitüberwachung öffentlicher Räume als Praktiken im Bereich der Künstlichen Intelligenz, die entweder ganz verboten sind oder nur unter sehr engen Ausnahmebedingungen zulässig.

3

1.3 Einsatzfelder ohne personenbezogene Daten?

Bei der Festlegung von Einsatzfeldern kann sich herausstellen, dass es abgrenzbare Einsatzbereiche gibt, in denen keinerlei personenbezogene Daten vorkommen, weder als Eingabedaten oder Ausgabedaten einer KI-Anwendung, noch im Anmelde- und Verarbeitungsprozess der KI-Anwendung. Solche Einsatzfelder unterliegen nicht dem Datenschutzrecht. Allerdings ist hierbei zu beachten, dass ein Personenbezug sich durch viele Merkmale, nicht nur durch Namen und Adressdaten ergeben kann. Die Prüfung, ob personenbezogene Daten in einem Einsatzfeld vorkommen oder nicht, ist daher gründlich und über den Lebenszyklus der Daten hinweg durchzuführen.

4

Beispiel 1: Ein geologisches Landesamt möchte mithilfe einer KI-Anwendung alte Rohstoffkartierungen neu bewerten. Hierbei werden nur geologische Karten verwendet, die keinen Personenbezug haben und sich auch nicht auf Gebiete mit Wohnbebauung beziehen.

5

Beispiel 2: Das Entwicklungsteam eines Unternehmens nutzt einen LLM-Chatbot, um Fehler in einer Code-Sequenz zu finden, die keinen Personenbezug enthält. Es ist

6

jedoch zu prüfen, ob eine Verarbeitung personenbezogener Daten aufgrund eines Personenbezugs im KI-Modell vorliegen kann.

1.4 Datenschutzkonformes Training von KI-Anwendungen

- 7 Hinsichtlich der Auswahl von KI-Anwendungen kann es eine Rolle spielen, ob und inwiefern KI-Anwendungen datenschutzkonform trainiert wurden.
 - Wurden für das Training personenbezogene Daten verwendet?
 - Falls ja, gab es eine Rechtsgrundlage für die Nutzung der Daten für das Training?
 - Inwiefern weist die KI-Anwendung zum Zeitpunkt des Einsatzes selbst Personenbezug auf?
- 8 Auf diese Parameter haben die Verantwortlichen, die KI-Anwendungen einsetzen, in der Regel keinen Einfluss. Verantwortliche, die KI in eigener Verantwortung einsetzen, müssen aber sicherstellen, dass sich Fehler beim Training einer KI-Anwendung nicht auf die Datenverarbeitung in ihrer Verantwortlichkeit auswirken.

1.5 Rechtsgrundlage für die Datenverarbeitung?

- 9 Für jeden Verarbeitungsschritt, bei dem mit Hilfe einer KI-Anwendung personenbezogene Daten verarbeitet werden, ist eine datenschutzrechtliche Rechtsgrundlage erforderlich. In Betracht kommen verschiedene Rechtsgrundlagen, je nachdem ob es sich um eine öffentliche oder nicht öffentliche Stelle handelt und ob es sich zum Beispiel um eine Anwendung auf dem Gebiet des Personalwesens, des Gesundheitswesens oder um eine Verarbeitung im Bereich eines Verbraucher:innen- oder Dienstleistungsvertrags handelt.
- 10 Überdies kann der Einsatz von KI-Anwendungen, die personenbezogene Daten von Bürger:innen verarbeiten, durch öffentliche Stellen je nach Intensität der Verarbeitung einer spezifischen Rechtsgrundlage bedürfen, die die Risiken für die Rechte und Freiheiten der betroffenen Personen, die von der Verarbeitung ausgehen, konkret adressiert.
- 11 Eine Übersicht über weitreichende Fragestellungen bei der Auswahl und hinsichtlich der Erfüllung datenschutzrechtlicher Rechtsgrundlagen im Zusammenhang mit dem Einsatz von KI-Anwendungen bietet zum Beispiel das Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ des

Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg.¹

1.6 Keine automatisierte Letztentscheidung

Entscheidungen mit Rechtswirkung dürfen gemäß Art. 22 Abs. 1 DS-GVO grundsätzlich nur von Menschen getroffen werden. Ausnahmen sind nur in bestimmten Fällen zugelassen, etwa bei einer Einwilligung der betroffenen Person. Erarbeitet eine KI-Anwendung Vorschläge, die für eine betroffene Person Rechtswirkung entfalten, muss das Verfahren so gestaltet werden, dass dem entscheidenden Menschen ein tatsächlicher Entscheidungsspielraum zukommt und nicht maßgeblich aufgrund des KI-Vorschlags entschieden wird. Unzureichende Personalressourcen, Zeitdruck und fehlende Transparenz über den Entscheidungsweg der KI-gestützten Vorarbeit dürfen nicht dazu führen, dass Ergebnisse ungeprüft übernommen werden. Eine lediglich formelle Beteiligung eines Menschen im Entscheidungsprozess ist nicht ausreichend.

12

Beispiel:

Eine KI-Anwendung wertet alle eingegangenen Bewerbungen auf eine ausgeschriebene Stelle aus und verschickt selbstständig die Einladungen zu den Vorstellungsgesprächen. Dies stellt einen Verstoß gegen Art. 22 Abs. 1 DS-GVO dar.

13

Bei öffentlichen Stellen gilt außerdem Folgendes: Der vollständig automatisierte Erlass eines Verwaltungsaktes ist in § 35a VwVfG geregelt. Liegen die Voraussetzungen vor, gilt Art. 22 Abs. 1 DS-GVO gemäß Art. 22 Abs. 2 lit. b DS-GVO nicht. Ein vollständig automatisierter Erlass eines Verwaltungsakts ist nur dann zulässig, wenn es sich um eine gebundene Entscheidung handelt und eine ausdrückliche Ermächtigungsgrundlage besteht. Sofern die öffentliche Stelle über einen Beurteilungsspielraum verfügt oder Ermessen ausübt, scheidet der vollständig automatisierte Erlass aus.

14

1.7 Geschlossenes oder offenes System?

Bei KI-Anwendungen kann zwischen geschlossenen und offenen Systemen unterschieden werden.

15

Bei geschlossenen Systemen erfolgt die Datenverarbeitung in einer eingegrenzten und technisch abgeschlossenen Umgebung. Außerdem hat nur ein bestimmter eng begrenzter Anwender:innenkreis Zugriff auf die KI-Anwendung. Die Kontrolle über die Ein- und Ausgabedaten liegt bei geschlossenen Systemen bei den Anwendenden. Es ist systemseitig nicht vorgesehen, dass die bei der Anwendung eingegebenen oder

16

¹ <https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/>.

entstehenden Daten vom Anbieter des Systems zum weiteren Training verwendet werden.

- 17 Anders verhält es sich mit offenen Systemen. Solche KI-Anwendungen werden vom Anbietenden zum Beispiel als Cloud-Lösung betrieben und sind über das Internet für einen unbestimmten Anwender:innenkreis zugänglich. Die Eingabedaten verlassen damit den geschützten Bereich der Anwender:in und können, je nach Konzeption der KI-Anwendung, von dieser auch für die Beantwortung von Anfragen anderer Anwender:innen verwendet werden. In diesem Fall besteht das Risiko, dass personenbezogene Daten zu anderen Zwecken weiterverarbeitet werden oder auch unbefugten Dritten zugänglich sind und ihnen gegenüber offengelegt werden. In diesem Zusammenhang sei auch auf mögliche Übermittlungen von Daten in Drittstaaten hingewiesen, da sie in solchen Konstellationen häufig anzutreffen sind. Für Drittstaatenübermittlungen sind die Regelungen in Kapitel V der DS-GVO zu berücksichtigen.
- 18 Ein Risiko besteht auch hinsichtlich dienstlicher Informationen, die nicht für die Öffentlichkeit bestimmt sind oder die als Verschlusssache eingestuft sind.
- 19 Offene Systeme können überdies Zugang zu weiteren Datenquellen wie dem offenen Internet haben und hierdurch Personenbezug von Daten herstellen oder die Informationen zu einer Person erweitern.
- 20 Technisch geschlossene Systeme sind daher aus datenschutzrechtlicher Sicht vorzugs-
würdig.

1.8 Transparenz

- 21 Der Einsatz von KI-Anwendungen stellt Verantwortliche hinsichtlich ihrer Informations- und Transparenzpflichten in mehrfacher Hinsicht vor besondere Herausforderungen. Sofern Verantwortliche eine KI-Anwendung nicht selbst entwickeln, müssen sie darauf achten, dass Ihnen vom Anbieter ausreichend Informationen zur Verfügung gestellt werden, um die Transparenzanforderungen der Art. 12 ff. DS-GVO umsetzen zu können. Dafür haben die Hersteller den KI-Anwendern entsprechende Dokumentationen bereitzustellen. Wird die KI-Anwendung zum Beispiel als Cloud-Lösung eingesetzt, ist der Auftragsverarbeiter gemäß Art. 28 Abs. 3 Satz 2 lit. e DS-GVO verpflichtet, den Verantwortlichen dabei zu unterstützen, den Rechten der betroffenen Person nachzukommen.
- 22 Zu den Informationen, über die die Verantwortlichen informieren und Auskunft erteilen müssen, zählen auch Angaben über die bei einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 DS-GVO involvierte

Logik sowie die Tragweite und die möglichen Auswirkungen für die betroffene Person. Der Begriff der automatisierten Entscheidung wird viele KI-Anwendungen erfassen, die selbst automatisiert Entscheidungen treffen oder deren Ergebnis Entscheidungen wesentlich beeinflusst.

Aus dem Begriff der „Logik“ lässt sich dabei mindestens schließen, dass eine Erläuterung der Methode der Datenverarbeitung bezogen auf die Funktionsweise des Programmablaufs im Zusammenhang mit der konkreten Anwendung vorzunehmen ist. Visualisierungen und interaktive Techniken können dabei helfen, die Komplexität der Logik auf ein verständliches Maß herunter zu brechen.

23

1.9 Transparenz und Wahlmöglichkeit hinsichtlich KI-Training

Es ist zu prüfen, ob Ein- und Ausgabedaten für das Training verwendet werden, diesbezüglich ausreichend informiert wird und die Möglichkeit eröffnet wird, die Nutzung der Daten für das Training auszuschließen. Sollte ein Ausschluss der Nutzung zu Trainingszwecken nicht möglich sein und sind personenbezogene Daten betroffen, ist für diesen Zweck eine Rechtsgrundlage erforderlich. Datenschutzrechtlich vorzugswürdig sind daher Anwendungen, die die Ein- und Ausgabedaten nicht zu Trainingszwecken verwenden.

24

1.10 Transparenz und Wahlmöglichkeit hinsichtlich Eingabe-Historie

Viele durch Texteingaben (Prompts) gesteuerte Dienste bieten an, die Eingaben zu speichern, um z. B. den Dialog zu einem Thema zu einem späteren Zeitpunkt wieder aufnehmen zu können oder an einer weiteren Optimierung des Prompts zu arbeiten. Hierdurch wird eine Historie der Eingaben einer Person angelegt. Insbesondere bei der gemeinsamen Nutzung durch mehrere Beschäftigte muss dies transparent kommuniziert werden und die Möglichkeit für die Nutzer:innen bestehen, selbst darüber zu entscheiden, ob die eigene Eingabe-Historie gespeichert wird.

25

1.11 Berichtigung, Löschung und weitere Betroffenenrechte

Verantwortliche müssen gewährleisten, dass betroffene Personen ihre Rechte auf Berichtigung gemäß Art. 16 DS-GVO und Löschung gemäß Art. 17 DS-GVO ausüben können. Für beide Rechte müssen organisatorische und technische Verfahren konzipiert werden, damit diese auch wirksam ausgeübt werden können. Dafür sind die Vorgaben der datenschutzkonformen Technikgestaltung umzusetzen.

26

Beim Einsatz von KI-Anwendungen kann es aus unterschiedlichen Gründen dazu kommen, dass unrichtige personenbezogene Daten verarbeitet werden. Viele Anbieter:innen von KI-Anwendungen (insbesondere LLM-Chatbots) weisen sogar

27

ausdrücklich darauf hin, dass Anwendende sich nicht auf die Richtigkeit der Ergebnisse verlassen können, sondern diese überprüfen müssen. Hinsichtlich personenbezogener Daten besteht bei Unrichtigkeit jedoch ein Recht der betroffenen Personen auf Berichtigung. Diese Berichtigung muss in einer KI-Anwendung umsetzbar sein, zum Beispiel durch Korrektur von Daten oder durch ein Nachtraining/Fine Tuning.

- 28 Machen betroffene Personen von ihrem Recht auf Löschung gemäß Art. 17 Abs. 1 DS-GVO Gebrauch, ist zu beachten, dass einige KI-Anwendungen gegebenenfalls durch die Verknüpfung unterschiedlicher Daten einen Personenbezug herstellen können. Es ist daher besonders wichtig, dass bei der Löschung personenbezogener Daten darauf geachtet wird, dass eine Wiederherstellung des Personenbezugs dauerhaft unmöglich ist. Dies kann je nach KI-Anwendung auf verschiedenen Wegen umgesetzt werden.
- 29 Das Unterdrücken von unerwünschten Ausgaben mittels nachgeschalteter Filter stellt zwar nicht generell eine Löschung im Sinne von Art. 17 DS-GVO dar. Denn die Daten, die nach einer bestimmten Eingabe zu einer bestimmten Ausgabe führen, könnten weiterhin personenbeziehbar für das KI-Modell verfügbar sein. Filtertechnologien können aber einen Beitrag dazu leisten, bestimmte Ausgaben zu vermeiden und damit den Rechten und Freiheiten der von einer bestimmten Ausgabe betroffenen Personen dienen.
- 30 Auch die weiteren Betroffenenrechte auf Einschränkung der Verarbeitung und auf Datenübertragbarkeit sowie das Widerspruchsrecht müssen bei der Gestaltung der KI-Anwendung berücksichtigt werden.

1.12 Datenschutzbeauftragte und Beschäftigtenvertretung einbinden

- 31 Betriebliche und behördliche Datenschutzbeauftragte sollten stets eingebunden werden, wenn Entscheidungen über KI-Anwendungen vorbereitet oder getroffen werden. Auch die Beteiligung von Betriebs- und Personalräten ist in Betracht zu ziehen und zu prüfen.

2. Implementierung von KI-Anwendungen

2.1 Verantwortlichkeit festlegen und verbindlich regeln

- 32 Verantwortlicher im Sinne der DS-GVO ist, wer über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Wird die KI-Anwendung von einer Stelle ausschließlich zu eigenen Zwecken auf eigenen Servern betrieben, ist diese Stelle in der Regel auch als alleiniger Verantwortlicher anzusehen.

Setzt eine Stelle zu eigenen Zwecken eine KI-Anwendung eines externen Anbieters zum Beispiel als Cloud-Lösung ein, agiert der externe Anbieter als verlängerter Arm im Auftrag des Verantwortlichen. Dann besteht zwischen dem Anbieter der Anwendung und dem Verantwortlichen häufig ein Auftragsverarbeitungsverhältnis gemäß Art. 28 f. DS-GVO mit der Folge, dass mit dem Anbieter eine Vereinbarung gemäß Art. 28 Abs. 3 DS-GVO abzuschließen ist.

Von einer gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO kann auszugehen sein, wenn zwei Stellen gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden, also eine gemeinschaftliche Entscheidung hierüber treffen. Eine gemeinsame Verantwortlichkeit kann aber auch vorliegen, wenn die beteiligten Stellen sich ergänzende Entscheidungen treffen und diese für die Verarbeitung in einer Weise erforderlich sind, dass sie einen spürbaren Einfluss auf die Bestimmung der Zwecke und Mittel der Verarbeitung nehmen. Ein wichtiges Kriterium für die Annahme einer gemeinsamen Verantwortlichkeit bei konvergierenden Entscheidungen ist insbesondere, ob die Verarbeitung ohne Beteiligung beider Stellen an den Zwecken und Mitteln nicht möglich wäre in dem Sinne, dass die Verarbeitungsvorgänge beider Parteien untrennbar miteinander verbunden sind. Dies kommt etwa bei Kooperationen mehrerer Stellen in Betracht, wenn eine KI-Anwendung mit unterschiedlichen Datensätzen gespeist oder trainiert oder auf der Plattform einer Stelle ihre KI-Anwendung von anderen Stellen zu neuen KI-Anwendungen weiterentwickelt wird. Es ist nicht erforderlich, dass der Verantwortliche tatsächlich Zugang zu den verarbeiteten Daten hat, um als gemeinsam Verantwortlicher eingestuft zu werden.

33

Die beteiligten Stellen haben gemäß Art. 26 Abs. 1 Satz 2 DS-GVO in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welchen Verpflichtungen der DS-GVO, insbesondere der Erfüllung der Betroffenenrechte und der Informationspflichten gemäß Art. 13 und 14 DS-GVO nachkommt.

34

Art. 26 DS-GVO stellt keine Rechtsgrundlage zur Verarbeitung personenbezogener Daten dar, sodass jeder Verantwortliche eine eigene Rechtsgrundlage zur Verarbeitung im Rahmen der gemeinsamen Verantwortlichkeit benötigt. Außerdem ist die Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen ein eigener Verarbeitungsvorgang und bedarf als solcher einer Rechtsgrundlage.

35

2.2 Interne Regelungen treffen

Ohne klare Regelungen, ob und wie KI-Anwendungen im Arbeitsalltag eingesetzt werden dürfen, besteht das Risiko, dass Beschäftigte KI-Anwendungen eigenmächtig und unkontrolliert nutzen. Es ist davon auszugehen, dass dies derzeit Realität in vielen Unternehmen und Behörden ist. Dies kann zu Datenschutzverstößen führen oder auch

36

zu anderen Schäden für die jeweilige Organisation. Daher sollten klare interne Weisungen erteilt und dokumentiert werden, ob, unter welchen Voraussetzungen und zu welchen konkreten Zwecken welche KI-Anwendungen eingesetzt werden dürfen. Konkrete Beispiele der zugelassenen und der untersagten Einsatzszenarien können bei der Verdeutlichung hilfreich sein und sind daher zu empfehlen.

- 37 Unabhängig davon, ob durch eine KI-Anwendung personenbezogene Daten (inklusive Nutzungsdaten von Beschäftigten) verarbeitet werden, bietet sich der Erlass einer Dienst-/Handlungsanweisung oder auch der Abschluss einer Dienst-/Betriebsvereinbarung zwischen Leitung und Personal-/Betriebsrat an. In jedem Fall sollte ein klarer Rahmen für den Einsatz von KI-Anwendungen vorgegeben werden. Dies gilt umso mehr, wenn personenbezogene Daten verarbeitet werden. In einigen Fällen wird die Einführung einer KI-Anwendung auch einen betrieblichen Mitbestimmungstatbestand erfüllen.

2.3 Datenschutz-Folgenabschätzung

- 38 Vor der Verarbeitung personenbezogener Daten ist eine generelle Bewertung (Vorabprüfung) des Risikos hinsichtlich der Art, des Umfangs, des Zwecks und der Umstände der Verarbeitung vorzunehmen.
- 39 Wird dabei festgestellt, dass die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO erforderlich. Beim Einsatz von KI-Anwendungen wird dies vielfach der Fall sein. Die Datenschutzaufsichtsbehörden veröffentlichen darüber hinaus zu Verarbeitungen, für die eine DSFA durchgeführt werden muss, sogenannte „Muss-Listen“² und Hinweise zur Abschätzung, in welchen Fällen auf die DSFA verzichtet werden kann.
- 40 Soweit der Verantwortliche nicht gleichzeitig Anbieter des KI-Systems ist, ist er zur Durchführung einer Risikobewertung bzw. einer DSFA auf Informationen des Anbietenden insbesondere zur Funktionsweise des Systems angewiesen. Daher ist bei der Auswahl und dem Erwerb einer KI-Anwendung darauf zu achten, dass diese Informationen vom Anbietenden bereitgestellt werden.

2.4 Beschäftigte schützen, betriebliche Accounts einrichten

- 41 Für die berufliche Nutzung von KI-Anwendungen durch Beschäftigte sollten von Arbeitgeber:innen Geräte und Accounts zur Verfügung gestellt werden. Beschäftigte sollten

² „Muss-Liste“ für den nichtöffentlichen Bereich: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf. Für den öffentlichen Bereich haben die Datenschutzaufsichtsbehörden eigene „Muss“-Listen veröffentlicht.

nicht eigenständig und unter Verwendung privater Accounts und Geräte mit KI-Anwendungen arbeiten müssen, da auf diese Weise Profile zu den jeweiligen Beschäftigten entstehen können.

Die Accounts sollten nicht die Namen einzelner Beschäftigter enthalten, soweit die KI-Anwendung nicht auf eigenen Servern betrieben wird. Soweit die E-Mail-Adresse abgefragt wird, ist die Angabe einer Funktions-E-Mail-Adresse des Unternehmens oder der Dienststelle geboten. Teilweise werden auch Mobilfunknummern bei der Registrierung verlangt. Auch hierfür ist ein Telefon vom Arbeitgeber bereitzustellen.

42

2.5 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Gemäß Art. 25 DS-GVO müssen Verantwortliche für Systeme, in denen personenbezogene Daten verarbeitet werden, technische und organisatorische Maßnahmen treffen, um die Datenschutzgrundsätze umzusetzen. In Betracht kommt eine datenschutzkonforme Gestaltung im Sinne von „data protection by design“ und „data protection by default“, die den Besonderheiten von KI-Systemen Rechnung trägt. Diese Vorgaben sind bereits bei der Konzeption des KI-Systems zu beachten. Dies kann je nach KI-Anwendung verschiedene Aspekte betreffen. Zum Beispiel können für Accounts, die Beschäftigte nutzen sollen, die Funktionen zur Nutzung von Eingaben für das KI-Training und zur Eingabe-Historie bereits bei Inbetriebnahme eines Accounts so gewählt werden, dass keine Eingabedaten zu Trainingszwecken verarbeitet werden und keine Eingabe-Historie über die Sitzung hinaus gespeichert wird. Auch dürfen zum Account gehörende Ausgabedaten nicht automatisch veröffentlicht werden.

43

2.6 Datensicherheit

KI-Anwendungen müssen als informationstechnische Systeme neben den datenschutzrechtlich erforderlichen technischen und organisatorischen Maßnahmen (insbesondere nach Artikel 25 und 32 DS-GVO) grundsätzlich auch diejenigen Anforderungen erfüllen, die generell für IT-Systeme gelten. Hierzu zählen insbesondere Kriterien wie Zuverlässigkeit und Bedienbarkeit genauso wie Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit sowie Resilienz).

44

Gelingt es Angreifer:innen, unberechtigt auf die KI-Anwendungen zuzugreifen, können sie gegebenenfalls bisherige Aktivitäten, persönliche Informationen und Geschäftsgeheimnisse in Erfahrung bringen.

45

Speziell für den Einsatz von KI-Anwendungen bietet zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI) umfangreiche Informationen zur Informationssicherheit an.³

2.7 Beschäftigte sensibilisieren

- 46 Beschäftigte sollten durch Schulungen, Leitfäden und Gespräche dahingehend sensibilisiert werden, ob und wie sie KI-Anwendungen nutzen sollen und dürfen.

2.8 Weitere Entwicklungen verfolgen

- 47 Sowohl im rechtlichen als auch im technischen Bereich müssen die Verantwortlichen die aktuellen Entwicklungen verfolgen, die Auswirkungen auf die Verarbeitung personenbezogener Daten und die notwendige Beherrschung des Risikos für die Rechte und Freiheiten natürlicher Personen haben. Dazu gehört die Prüfung, inwieweit zusätzliche Anforderungen aus der europäischen KI-Verordnung erfüllt werden müssen. Auch in Bezug auf technische Entwicklungen, die sich auf das Risiko auswirken können, wie fortschreitende technische Lösungen und Updates sollte regelmäßig überprüft werden, ob die internen Vorgaben angepasst werden müssen. Hierzu sollte eine Routine im Rahmen des betrieblichen bzw. behördlichen Datenschutzmanagements (Art. 24 DS-GVO) etabliert werden.

3. Nutzung von KI-Anwendungen

3.1 Vorsicht bei Eingabe und Ausgabe personenbezogener Daten

- 48 Handelt es sich bei den Eingabedaten um personenbezogene Daten, sind betroffene Personen über die Verwendung ihrer Daten transparent zu informieren. Für die Verarbeitung personenbezogener Daten in KI-Anwendungen und die evtl. erfolgende Übermittlung dieser Daten an Anbieter von KI-Anwendungen muss außerdem jeweils eine Rechtsgrundlage erfüllt werden.
- 49 Um die Eingabe personenbezogener Daten zu vermeiden, reicht es regelmäßig nicht, Namen und Anschriften einer Eingabe zu entfernen. Gegebenenfalls lässt sich aus dem Zusammenhang ein Personenbezug zu betroffenen Personen herstellen. Bei KI-Anwendungen, deren Bestimmung es ist, Querbezüge auch aus unstrukturierten Daten herzustellen, ist diese Gefahr besonders hoch.

³ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html.

Beispiel einer Eingabe mit Personenbezug:

„Entwirf ein Arbeitszeugnis im befriedigenden Bereich für einen Kundenberater im Autohaus X.“ 50

Die Eingabe kann Personenbezug aufweisen, wenn erkennbar ist, aus welchem Unternehmen sie zu welchem Zeitpunkt getätigt wurde. 51

Auch wenn eine Eingabe keine personenbezogenen Daten enthält, kann die KI-Anwendung eine Ausgabe mit personenbezogenen Daten generieren. In solchen Fällen kann eine Rechtsgrundlage erforderlich sein. Zudem ist zu prüfen, ob die betroffenen Personen gemäß Art. 14 DS-GVO über die Verarbeitung informiert werden müssen. Dies ist zumindest dann erforderlich, wenn die Anfrage auf einen Personenbezug abzielte oder die personenbezogene Ausgabe weiterverarbeitet werden soll. 52

Beispiel 1 einer Eingabe, die eine Ausgabe ohne Personenbezug produziert:

Eingabe: 53
„Nenne zwei Romane von Hermann Hesse.“

Ausgabe: 54
„Zwei Romane von Hermann Hesse sind:
1. "Siddhartha" (1922): Ein philosophischer Roman, der die spirituelle Suche eines jungen Brahmanen namens Siddhartha im antiken Indien beschreibt.
2. "Der Steppenwolf" (1927): Ein psychologischer Roman, der die innere Zerrissenheit und Suche nach Identität eines Mannes namens Harry Haller in der modernen Welt thematisiert.“

Die Ausgabe enthält keine Daten lebender/echter Personen. 55

Beispiel 2 einer Eingabe, die eine Ausgabe ohne Personenbezug produziert:

Eingabe: 56
„Schreibe ein Haiku über Datenschutz.“

Ausgabe: 57
*„Daten geschützt fein,
Privatsphäre bleibt gewahrt,
Sicherheit im Netz.“*

Beispiel 3 einer Eingabe, die eine Ausgabe ohne Personenbezug produziert:

58 Eingabe:

„Nenne die ersten drei Elemente des Periodensystems.“

60 Ausgabe:

„Die ersten drei Elemente des Periodensystems sind Wasserstoff (H), Helium (He) und Lithium (Li).“

Beispiel einer Eingabe, die eine Ausgabe mit Personenbezug produziert:

61 *Der Fußballtrainer bittet eine KI: „Schlage mir die besten Spieler für die Aufstellung vor.“*

3.2 Besondere Vorsicht bei besonderen Kategorien personenbezogener Daten

62 Besondere Kategorien personenbezogener Daten sieht der Unionsgesetzgeber als besonders schutzwürdig an. Dazu gehören etwa personenbezogene Daten aus denen religiöse oder weltanschauliche Überzeugungen, eine Gewerkschaftszugehörigkeit oder die Präferenz für eine bestimmte politische Partei hervorgehen sowie Gesundheitsdaten, genetische oder biometrische Daten. Hierunter fallen z. B. die Einnahme bestimmter Medikamente oder der regelmäßige Besuch einer bestimmten Kirche. Die Verarbeitung solcher Daten ist gemäß Art. 9 Abs. 1 DS-GVO grundsätzlich verboten und nur ausnahmsweise unter den Voraussetzungen des Art. 9 Abs. 2 bis 4 DS-GVO erlaubt. Diesbezüglich ist also sowohl hinsichtlich der Eingabe als auch hinsichtlich der Verarbeitung und der Ausgabe besonders geschützter Daten zu prüfen, ob eine der Ausnahmen des Art. 9 Abs. 2 DS-GVO erfüllt ist.

Beispiel:

63 In der Hautdiagnostik, insbesondere bei der Krebsfrüherkennung in der Arztpraxis, spielt der Einsatz von KI-basierten Systemen eine wichtige Rolle und ergänzt die ärztliche Diagnostik. Entspricht eine KI-Anwendung dem fachlichen Standard und ist als Medizinprodukt zugelassen, kann Art. 9 Abs. 2 lit. h DS-GVO i. V. m. dem Behandlungsvertrag für die Verarbeitung der Patientendaten geeignet sein. Anderenfalls kommt eine informierte ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht, der Informationen und Erklärungen über die spezifische Funktionsweise der KI-Anwendung vorausgehen müssen.

3.3 Ergebnisse auf Richtigkeit prüfen

64 Die Ergebnisse von KI-Anwendungen mit Personenbezug müssen kritisch hinterfragt werden. Insbesondere die Anbietenden von LLM stellen häufig klar, dass die mit ihrer

Anwendung erzeugten Texte keinen Anspruch auf Richtigkeit haben und stets hinterfragt werden sollten. Überdies können KI-Anwendungen unterschiedliche Informationsstände haben.

Im Hinblick auf personenbezogene Ergebnisse oder eine personenbezogene Anwendung der Ergebnisse können unrichtige Ergebnisse aber zu unzulässigen Verarbeitungen führen, so dass vor der Weiterverarbeitung eine Überprüfung erfolgen muss.

65

3.4 Ergebnisse und Verfahren auf Diskriminierung prüfen

Auch unabhängig von ihrer sachlichen Richtigkeit oder ihrem eigenen Personenbezug können Ergebnisse von KI-Anwendungen zu unzulässigen Verarbeitungen personenbezogener Daten führen, z. B. wenn sie diskriminierend wirken. Eine darauf aufbauende Datenverarbeitung kann unzulässig sein, wenn sie beispielsweise bezweckt, gegen das Allgemeine Gleichbehandlungsgesetz (AGG) zu verstoßen und deshalb die Rechtsgrundlage des Art. 6 Abs. 1 lit. f DS-GVO nicht erfüllt. Die Verantwortlichen müssen daher prüfen, ob Ergebnisse einer KI-Anwendung für die weitere Verwendung im gesetzlichen Rahmen tragbar sind.

66

Auch wenn Diskriminierungen in einzelnen Ergebnissen nicht erkennbar sind, können diese diskriminierend wirken.

67

Beispiel:

Eine KI-Anwendung könnte anhand früherer erfolgreicher Bewerbungen in einem Unternehmen folgende Empfehlung geben: *„Für die freie Stelle sollten bevorzugt männliche Bewerber ausgewählt werden.“*

68

Die Anwendung dieses Ergebnisses auf Bewerber:innen in einem Bewerbungsverfahren würde eine unzulässige Verarbeitung der Geschlechtsangaben der Bewerber:innen darstellen, da sie gegen § 7 Abs. 1 i. V. m. § 1 Abs. 1 AGG verstoßen würde, indem sie nicht männliche Personen benachteiligt.

69