BLM
DER MEDIEN-
BEAUFTRAGTE
FÜR DEN
DATENSCHUTZ

MERKBLATT

Datenschutzrechtliche Anforderungen an den Einsatz von KI

Stand: April 2026

Vorüberlegungen

1. Einsatzfelder und Zwecke bestimmen

- Welche Einsatzfelder sind für die KI-Anwendung vorgesehen?
- Welchem Zweck soll die KI konkret dienen?

2. Sind die Einsatzfelder rechtmäßig

- Der Einsatz von KI in bestimmten Einsatzfeldern (zum Beispiel „Social Scoring“) ist generell unzulässig (vergleiche Artikel 5 KI-Verordnung).

3. Einsatzfelder ohne personenbezogene Daten

- Wenn tatsächlich keinerlei personenbezogene Daten in der KI verarbeitet werden, also solche weder beim Training verwendet wurden noch beim Einsatz in die KI-Anwendung eingegeben werden, sind keine datenschutzrechtlichen Bestimmungen einschlägig.
- Denkbar ist dies, zum Beispiel bei spezialisierten KI-Systemen, die nur mit „technischen Daten“ wie zum Beispiel Wetterdaten, Finanzdaten, Software-Code oder Ähnlichem trainiert wurden und in diesen Bereichen eingesetzt werden (zum Beispiel als Wetter-KI, Finanz-KI, Coding-KI).
- In den üblichen Fällen wird aber in der Regel nicht auszuschließen sein, dass personenbezogene Daten zumindest während des Trainings verwendet wurden. Daher ist diese Frage eingehend zu prüfen.

Werden im Rahmen einer KI-Anwendung personenbezogene Daten verarbeitet, sind in datenschutzrechtlicher Hinsicht folgende Fragen zu beantworten bzw. Anforderungen zu erfüllen:

Rechtliche Vorgaben für die Konzeption von KI-Anwendungen

Zweck der Datenverarbeitung bestimmen

1.

- Ausgangspunkt datenschutzrechtlicher Erwägungen ist in der Regel der vorgesehene Zweck der Datenverarbeitung.
- Dieser kann zur Zulässigkeit der Datenverarbeitung führen, wenn für den Zweck eine Rechtsgrundlage, wie zum Beispiel aus Artikel 6 Absatz 1 DS-GVO, besteht und die Datenverarbeitung zur Zweckerreichung erforderlich ist.

Fragen zum Training der einzusetzenden KI beantworten

2.

- Wurden für das Training personenbezogene Daten verwendet?
- Falls ja, gab es eine Rechtsgrundlage für die Nutzung der Daten für das Training?
- Zudem ist zu bedenken, dass die Verantwortlichen, die KI nur einsetzen (und nicht selbst entwickeln/entwickeln lassen) und deshalb auf das Training keinen Einfluss nehmen können, sicherstellen müssen, dass sich Fehler beim Training einer KI-Anwendung nicht auf die Datenverarbeitung in ihrer Verantwortlichkeit auswirken.

Rechtsgrundlage für die Datenverarbeitung (innerhalb der KI)

3.

- Jeder Verarbeitungsschritt innerhalb oder mittels der KI bedarf einer datenschutzrechtlichen Rechtsgrundlage, wenn dort personenbezogene Daten verarbeitet werden.

Keine automatisierte Letztentscheidung

4.

- KI-Anwendungen dürfen keine Entscheidung mit Rechtwirkung auslösen, Artikel 22 Absatz 1 DS-GVO. Das wäre zum Beispiel bei einer Bewerbungssoftware der Fall, die automatisiert Bewerbungen aussortiert, so dass diese der Personalabteilung nie angezeigt werden.
- Soll die KI eine Entscheidung vorbereiten, muss der Entscheidungsprozess so ausgestaltet sein, dass die Letztentscheidung tatsächlich bei einer Person verbleibt.

Geschlossenes oder offenes System

5.

- Beim Einsatz von geschlossenen Systemen liegt die Kontrolle über die Ein- und Ausgabedaten beim Anwender, der allein über die Verarbeitungszwecke und auch den Einsatz zu Trainingszwecken entscheidet.
- Bei offenen Systemen (zum Beispiel in der Cloud) ist dies nicht der Fall; sie verlassen den geschützten Bereich des Anwenders, so dass das Risiko besteht, dass personenbezogene und gegebenenfalls auch betriebliche Daten zu anderen Zwecken weiterverarbeitet oder auch unbefugten Dritten zugänglich oder ihnen gegenüber offengelegt werden.
- Diesen Risiken ist entsprechend zu begegnen; geschlossene Systeme sind daher vorzugswürdig und werfen weniger Fragen auf.

Informationsgrundlage

6.

- Anwender benötigen hinreichende Informationen vom Entwickler der KI-Anwendung (unter anderem zu den verwendeten Trainingsdaten, Sicherheitsvorkehrungen, Manipulationsgefahren etc.), damit sie die Transparenzanforderungen der Artikel 12 DS-GVO ff. umsetzen können.

Transparenz und Wahlmöglichkeit hinsichtlich KI-Training

7.

- Anwender müssen prüfen, ob Ein- und Ausgabedaten für das Training verwendet werden.
- Sollte ein Ausschluss der Nutzung zu Trainingszwecken nicht möglich sein und sind personenbezogene Daten betroffen, ist für diesen Zweck eine Rechtsgrundlage erforderlich.

Transparenz und Wahlmöglichkeit hinsichtlich Eingabe-Historie

8.

- KI-Anwendungen bieten in der Regel eine Historie an, so dass die bisherigen Ein- und Ausgaben gespeichert werden.
- Insbesondere bei der gemeinsamen Nutzung durch Mehrere muss transparent hierüber informiert und idealerweise jedem Nutzer die Möglichkeit eingeräumt werden zu entscheiden, ob eine Historie angelegt wird.

Berichtigung, Löschung und weitere Betroffenenrechte

9.

- Betroffenenrechte müssen gewährleistet werden, insbesondere das Recht auf Berichtigung wie auch auf Löschung.
- Hierzu müssen technische und organisatorische Verfahren konzipiert werden, damit die genannten Rechte auch wirksam ausgeübt werden können.
- Auch wenn sich Anwender nicht auf die Richtigkeit der Ergebnisse einer KI-Anwendung verlassen können, haben betroffene Personen bei Unrichtigkeit ihrer personenbezogenen Daten ein Recht auf Berichtigung dieser Daten. Dies muss umsetzbar sein zum Beispiel durch Korrektur von Daten oder durch Nachtraining/Fine Tuning.
- Bei der Löschung personenbezogener Daten ist darauf zu achten, dass eine Wiederherstellung des Personenbezugs dauerhaft unmöglich ist.
- Unterdrücken von unerwünschten Ausgaben mittels nachgeschalteter Filter führt nicht zur Löschung der Daten im Sinne von Artikel 17 DS-GVO, da die Daten weiterhin für das Modell verfügbar bleiben. Gleichwohl kann das Vermeiden bestimmter Ausgaben aber einen Beitrag leisten, die Rechte und Freiheiten der betroffenen Personen zu stärken.

Datenschutzbeauftragte und Beschäftigtenvertretung einbinden

10.

- Vor dem Einsatz von KI-Anwendungen sollten – wie bei anderen technischen Tools auch – der Datenschutzbeauftragte sowie gegebenenfalls auch die Beschäftigtenvertretung eingebunden werden.

Vorgaben und Hinweise für die Implementierung von KI-Anwendungen

Verantwortlichkeiten festlegen und verbindlich regeln

1.

- Verantwortlicher im Sinne der DS-GVO ist, wer über Zwecke und Mittel der Verarbeitung entscheidet. Wenn KI-Anwendungen auf eigener Infrastruktur zu eigenen Zwecken betrieben werden, ist diese Stelle in der Regel der alleinige Verantwortliche.
- Wenn KI-Anwendungen von externen Anbietern eingesetzt werden (zum Beispiel als Cloud-Lösungen), liegt in der Regel ein Auftragsverarbeitungsverhältnis nach Artikel 28 DS-GVO vor, wenn der externe Anbieter nur das erledigt, was ihm vom Anwender/Verantwortlichen aufgetragen wurde. Hierzu muss ein entsprechender Auftragsverarbeitungsvertrag zwischen dem Anwender/Verantwortlichen und dem externen Anbieter geschlossen werden.
- Wenn der Anwender und der externe Anbieter gemeinsam über Zwecke und Mittel der Verarbeitung entscheiden, kann von einer gemeinsamen Verantwortlichkeit gemäß Artikel 26 DS-GVO ausgegangen werden. Auch hier muss eine transparente Vereinbarung getroffen werden, die die Verantwortlichkeiten regelt.
- Artikel 26 DS-GVO stellt keine eigene Rechtsgrundlage dar, sodass jeder der gemeinsam Verantwortlichen (Anwender und externe Anbieter) eine eigene Rechtsgrundlage benötigt. Darüber hinaus bedarf auch die Übermittlung personenbezogener Daten zwischen gemeinsam Verantwortlichen jeweils einer eigenen Rechtsgrundlage, da dies einen eigenen Verarbeitungsvorgang darstellt.

Klare interne Regelungen treffen

2.

- Man sollte klare interne Weisungen erteilen und dokumentieren, ob, unter welchen Voraussetzungen und zu welchen konkreten Zwecken welche KI-Anwendungen eingesetzt werden dürfen.

Datenschutzfolgen-abschätzung

3.

- Vor der Verarbeitung personenbezogener Daten ist eine Vorabprüfung des Risikos für betroffene Personen vorzunehmen.
- Eine Datenschutzfolgenabschätzung (DSFA) nach Artikel 35 DS-GVO ist erforderlich, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen von der Verarbeitung ausgeht.
- Bei Einsatz von KI-Anwendungen wird dies häufig der Fall sein.

Beschäftigte schützen, betriebliche Accounts einrichten

4.

- Für die berufliche Nutzung von KI durch Beschäftigte sollte der Arbeitgeber entsprechende Betriebsmittel (insbesondere Endgeräte, Accounts, ...) zur Verfügung stellen, um die ungewollte Verarbeitung von Daten der Beschäftigten insbesondere durch Dritte zu verhindern.
- Bei privaten Accounts ist die Gefahr höher, dass die vom Nutzer eingegebenen Informationen durch den Anbieter der KI-Anwendung auch zu anderen Zwecken verwendet werden, da der Ausschluss der Nutzung von Ein- und Ausgaben zu anderen und insbesondere Trainingszwecken zumeist nur bei Business Accounts möglich ist.
- Der Einsatz von Funktionsemailadressen ist in der Regel sinnvoll und daher zu empfehlen.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

5.

- Data Protection by Design und Data Protection by Default sollten – idealerweise bereits bei der Konzeption des KI-Systems – beachtet werden.
- Schon bei der Inbetriebnahme eines KI-Systems kann so unter anderem das Training anhand der Ein- und Ausgabedaten deaktiviert und die Speicherung der Eingabe-Historie auf die aktuelle Session beschränkt werden.

Datensicherheit

6.

- KI-Systeme müssen jenseits der in Artikel 25 und 32 DS-GVO vorgegebenen, datenschutzrechtlichen, technischen und organisatorischen Maßnahmen auch alle anderen für IT-Systeme geltenden Sicherheitsanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit sowie Resilienz) erfüllen.

Beschäftigte sensibilisieren

7.

- Beschäftigte sollten zur Frage, ob und wie sie KI-Anwendungen nutzen können und dürfen, sensibilisiert und geschult werden.

Weitere Entwicklungen verfolgen

8.

- KI-Anwendungen haben häufig Auswirkungen auf die Rechte und Freiheiten der Betroffenen.
- Um diese Risiken zu beherrschen, müssen Verantwortliche die aktuellen rechtlichen und technischen Entwicklungen verfolgen.
- Technische Einstellungen und Vorgaben sind insoweit regelmäßig zu überprüfen.

Empfehlungen für den Einsatz von KI-Anwendungen

Vorsicht bei Eingabe und Ausgabe personenbezogener Daten

1.

- Wenn es sich bei Eingabedaten um personenbezogene Daten handelt, sind betroffene Personen über die Verwendung ihrer Daten transparent zu informieren.
- Entfernen von Namen und Anschrift während der Eingabe reicht regelmäßig nicht aus, da sich der Personenbezug gegebenenfalls aus dem Zusammenhang ergeben kann.
- Bei KI-Systemen besteht zudem die Gefahr, dass diese aufgrund von Inferenzen Personenbezüge herstellen können (das heißt auch wenn gar keine personenbezogenen Daten eingegeben wurden, können die Systeme aufgrund der Umstände einen Personenbezug herstellen).

Besondere Vorsicht bei personenbezogenen Daten besonderer Kategorien

2.

- Die Verarbeitung bestimmter Kategorien personenbezogener Daten (vergleiche Artikel 9 Absatz 1 DS-GVO) gilt als besonders sensibel, ist daher prinzipiell verboten und nur ausnahmsweise erlaubt (Artikel 9 Absatz 2 bis 4 DS-GVO).
- Deshalb ist bei der Verarbeitung dieser Daten besondere Vorsicht geboten.

Ergebnisse auf Richtigkeit überprüfen

3.

- Ausgaben von KI-Anwendungen können – aus verschiedenen Gründen – unrichtig sein. Deshalb müssen Ergebnisse mit Personenbezügen kritisch hinterfragt werden.
- Wenn mit solchen unrichtigen Ergebnissen weitergearbeitet wird, kann dies zu einer unzulässigen Verarbeitung führen, sodass stets eine Überprüfung vor der Weiterverarbeitung erfolgen muss.

Ergebnisse und Verfahren auf Diskriminierung prüfen

4.

- Jenseits von unrichtigen personenbezogenen Daten kann eine Verarbeitung unzulässig sein, wenn sie diskriminierend wirkt.
- Dies kann dann vorliegen, wenn eine KI-Anwendung eingesetzt wird und zum Beispiel Bewerber eines Geschlechts bevorzugt oder besser bewertet werden.