PerspektiveArbeit
Lausitz

Rechtlicher Leitfaden zur Nutzung von KI-Systemen in Unternehmen

Zwickau, 01.03.2026

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt

Das zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt unter den Förderkennzeichen 02L19C300 - 02L19C333 gefördert. Projektlaufzeit: 01.11.2021 – 31.10.2026

Inhalt

Impressum

Herausgeber:
Westsächsische Hochschule Zwickau, PÜHN Rechtsanwälte

Redaktion/Autoren:
R. Junghanns, A. Freier, S. Junghans, F. Dietrich
Bildnachweis:
pixabay.com, freepik.com, PowerPoint

1. Auflage 2026

Kompetenzzentren Arbeitsforschung

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Das zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 02L19C300 - 02L19C333 gefördert. Projektlaufzeit: 01.11.2021 – 31.10.2026

Vorwort

Liebe Personalverantwortliche und Führungskräfte,

Forschung ist zukunftsorientiert – und die Zukunft der modernen Arbeitswelt wird in vielen Bereichen untrennbar mit künstlicher Intelligenz (KI) verbunden sein. Werden personenbezogene Daten in Systemen der künstlichen Intelligenz verarbeitet, bilden die **Datenschutz-Grundverordnung (DS-GVO)** , das **Bundesdatenschutzgesetz (BDSG)** und die **Europäische Verordnung über künstliche Intelligenz (KI-VO)** - auch AI Act genannt - die zentralen rechtlichen Rahmenbedingungen. Von der verfahrensbezogenen DS-GVO, die durch nationale Regelungen im BDGS konkretisiert wird, unterscheidet sich grundlegend die KI-VO als produktbezogene Softwareregulierung. Diese beiden Regularien – insbesondere die Frage, *wer* Pflichten zu erfüllen und *was* zu gewährleisten hat – werden in diesem Leitfaden dargestellt.

Die Forschungsgruppe stellt eingangs klar, dass der rechtliche Rahmen für den Einsatz von KI – entgegen häufig geäußerter Kritik – nicht als Behinderung, sondern als notwendiger Schritt verstanden wird. Er dient dazu, zu regeln, wie wir als moderne Gesellschaft künftig zusammenleben wollen. Eine technikoffene, freiheitlich orientierte Gesellschaft setzt die Achtung und den Schutz des individuellen Rechts auf informationelle Selbstbestimmung voraus.

Die Forschungsprojekte verfolgen von Beginn an den Grundsatz Privacy by Design. Dieser Ansatz gewährleistet eine klare rechtliche Umsetzbarkeit für spätere Wirtschaftsakteure und begründet zugleich Wettbewerbsvorteile.

Quelle: Pixabay

Einleitung

Quelle: Freepik

Problemstellung & Relevanz:

Der Einsatz von KI bietet Unternehmen große Chancen, etwa durch Automatisierung und effizientere Entscheidungen. Gleichzeitig steigt jedoch die Komplexität rechtlicher Anforderungen – von Datenschutz und Urheberrecht über Haftungsfragen bis hin zu neuen Vorgaben wie der KI-VO. Ein kompakter rechtlicher Leitfaden schafft Orientierung, reduziert Unsicherheiten und unterstützt einen verantwortungsvollen, rechtssicheren KI-Einsatz.

Zielgruppe:

Dieser Leitfaden richtet sich an Personalverantwortliche und Führungskräfte in Unternehmen, in denen KI zum Einsatz kommt.

Das erwartet Sie:

In diesem Leitfaden werden die grundlegenden Anforderungen und Pflichten für Unternehmen beschrieben, die sich aus der DS-GVO, dem BDSG und der KI-VO ergeben. Um das Verständnis und die praktische Anwendung zu erleichtern, werden die theoretischen Inhalte mit Beispielen eines Arbeitgebers, der KI einsetzen möchte, verknüpft.

Praxisbeispiel

Das Projekt „KI-gestütztes Onboarding“

Ein Arbeitgeber muss ein schnelles und sicheres Onboarding neuer Mitarbeiter gewährleisten. Er beauftragt einen externen Dienstleister, Praxiswissen erfahrener Mitarbeiter - zugeordnet nach Arbeitsplätzen, Abteilungen oder Aufgaben im Unternehmen - zu sammeln; KI-gestützt fachlich und methodisch aufzubereiten, um dieses Wissen neuen Mitarbeitern zur Einarbeitung und digitaler Schulung mit individueller KI-gesteuerter Lernfortschrittskontrolle modern und mehrsprachig zur Verfügung zu stellen und um gleichzeitig Belastungsspitzen entgegenzuwirken und ein gesundes Arbeitsumfeld zu fördern.

Quelle: Freepik

Teil 1: DS-GVO / BDSG

Die DS-GVO ist eine EU-weite Verordnung zum Schutz personenbezogener Daten (z. B. Beschäftigtendaten). Das BDSG ergänzt die DS-GVO in Deutschland mit nationalen Datenschutzregelungen.

1. Datenschutzrechtliche Grundlagen

Personenbezogene Daten und Verarbeitung

Personenbezogene Daten umfassen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Verarbeitung umfasst jeden Umgang mit diesen Daten - vom Erheben über die Speicherung bis hin zur Analyse durch KI-Systeme. Für Beschäftigtendaten gelten zudem spezielle Anforderungen gemäß § 26 BDSG, um Nachteile für die Mitarbeiter zu vermeiden. Besondere Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, erfordern einen erhöhten Schutz gemäß Art. 9 DS-GVO.

Die Anonymisierung von Daten ist nicht nur soweit möglich geboten, sondern zugleich ein probates Mittel des Risikomanagements, da ihre weitere Verarbeitung dann keinen datenschutzrechtlichen Restriktionen mehr unterliegt.

Rollen und Verantwortlichkeiten

Eine klare Rollenbestimmung ist fundamental. Der Verantwortliche für die Datenverarbeitung ist das Unternehmen, das über die Zwecke und Mittel der Datenverarbeitung entscheidet. Sofern ein Dienstleister hinzugezogen wird und über die „wesentlichen" Mittel der Verarbeitung mitentscheidet, gilt er zusammen mit dem Unternehmen als gemeinsam Verantwortlicher gemäß Art. 26 DS-GVO; andernfalls fungiert er als Auftragsverarbeiter.

Die einzelnen datenschutzrechtlichen Pflichten sind sowohl zwischen mehreren Verantwortlichen als auch im Verhältnis zu Auftragsverarbeitern vertraglich transparent zuzuweisen bzw. deren Durchsetzung vertraglich zu sichern.

Empfehlungen

- ✓ Identifizieren Sie den betroffenen Personenkreis und die Kategorien personenbezogener Daten in den jeweiligen Verarbeitungsschritten.
- ✓ Definieren und dokumentieren Sie Verantwortlichkeiten klar.
- ✓ Führen Sie für jeden Verantwortlichen ein Verzeichnis aller Verarbeitungstätigkeiten, die dessen Zuständigkeit unterliegen.
- ✓ Schließen Sie erforderliche Verträge mit Dienstleistern ab. Nutzen Sie anerkannte und aktuelle Muster.
- ✓ Etablieren Sie Prozesse zur Datenanonymisierung.

Quelle: Pixabay

Teil 1: DS-GVO / BDSG

Praxisbeispiel

Der Verarbeitungsprozess des Projekts „KI-gestütztes Onboarding“ wird in zwei klar voneinander getrennte Abschnitte unterteilt:

(1) die Erfassung und Aufbereitung des Praxiswissens erfahrener Mitarbeitender („Wissensgeber“) und

(2) das KI-gestützte Onboarding neuer Mitarbeitender mit individueller Lernfortschrittskontrolle.

Es werden personenbezogene Daten der erfahrenen Beschäftigten („Wissensgeber“) und der neuen Mitarbeitenden verarbeitet.

Die Wissensgeber stellen ihr Fachwissen zur Verfügung, das durch den externen KI-Dienstleister strukturiert, aufbereitet und in Lerninhalte überführt wird. Dabei werden – soweit möglich – keine personenbezogenen Daten, sondern anonymisierte oder aggregierte Wissensinhalte verwendet.

Die neuen Mitarbeitenden nutzen das KI-System zur Einarbeitung. Dabei werden u.a. Name, Funktion, Abteilung, Spracheinstellung, Lernfortschritte, Testergebnisse und Interaktionen mit dem System verarbeitet.

Das Unternehmen, dass über den Zweck der Datenverarbeitung entscheidet, und der hinzugezogene Dienstleister, der über das entsprechende Know-how verfügt und somit über die "wesentlichen" Mittel der Datenverarbeitung – Einsatz und Ausgestaltung der KI zur Datenerfassung und zur Schulung/Onboarding - entscheidet, sind "gemeinsame Verantwortliche„...

...Zwischen dem Unternehmen und dem externen Dienstleister wird daher eine Vereinbarung über gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO (Joint Controller Vereinbarung) abgeschlossen. In dieser Vereinbarung wird verbindlich festgelegt:

- welche Partei welche datenschutzrechtlichen Pflichten erfüllt,
- wie Betroffenenrechte gewährleistet werden und
- welche Kontroll- und Durchsetzungsrechte dem Unternehmen gegenüber dem Dienstleister zustehen.

Die wesentlichen Inhalte dieser Joint-Controller-Vereinbarung werden den betroffenen Mitarbeitenden zur Verfügung gestellt.

Der Datenschutzbeauftragte des Unternehmens – je nachdem, ob gesetzlich verpflichtend oder fakultativ berufen – und der Betriebsrat werden frühzeitig eingebunden.

Teil 1: DS-GVO / BDSG

2. Grundsätze der Verarbeitung gemäß Art. 5 DS-GVO

Empfehlungen

- ✓ Entwickeln (und aktualisieren) Sie Richtlinien zur Erfassung und Verarbeitung personenbezogener Daten.

Praxisbeispiel

Beim Einsatz des KI-Onboarding-Systems stellt das Unternehmen sicher, dass die Verarbeitung der Daten der Wissensgeber und der neuen Mitarbeitenden rechtmäßig, zweckgebunden, transparent und auf das notwendige Maß beschränkt erfolgt...

...Die erhobenen Informationen werden ausschließlich für die strukturierte Wissensvermittlung, die Erstellung individueller Lernpfade und die Begleitung des Einarbeitungsprozesses verwendet.

Das Unternehmen legt dem externen KI-Dienstleister vertraglich verbindliche Vorgaben zur Datenminimierung fest. Der Dienstleister darf nur diejenigen personenbezogenen Daten verarbeiten, die für den Betrieb des KI-gestützten Onboardings zwingend erforderlich sind. Eine darüberhinausgehende Nutzung, etwa für allgemeines KI-Training oder andere Zwecke, ist ausgeschlossen.

Das Praxiswissen der erfahrenen Mitarbeitenden wird – soweit technisch möglich – anonymisiert oder aggregiert, bevor es in das KI-System einfließt.

Lernfortschritts- und Profildaten der neuen Mitarbeitenden werden regelmäßig überprüft und gelöscht, sobald sie für das Onboarding nicht mehr erforderlich sind.

Teil 1: DS-GVO / BDSG

3. Schwerpunkt: Rechtmäßigkeit der Verarbeitung

Nach Art. 6 Abs. 1 der DS-GVO ist die Verarbeitung personenbezogener Daten nur zulässig, wenn mindestens eine der darin genannten Bedingungen erfüllt ist:

- Einwilligung der betroffenen Person
- Erforderlichkeit zur Vertragserfüllung
- Erfüllung einer rechtlichen Verpflichtung
- Schutz lebenswichtiger Interessen
- Wahrnehmung von Aufgaben des öffentlichen Interesses oder in Ausübung öffentlicher Gewalt
- Wahrung berechtigter Interessen des Verantwortlichen oder Dritter

Im Beschäftigungskontext ist insbesondere die Einwilligung der Beschäftigten von Bedeutung (Art. 6 Abs. 1 a) DS-GVO, § 26 Abs. 2 BDSG* und Art. 9 Abs. 2 a) DS-GVO) für Gesundheitsdaten sowie § 25 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten).

Die Einwilligung muss folgende Anforderungen erfüllen:

- freiwillig, informiert, spezifisch und jederzeit widerrufbar (Art. 4 Nr. 11 und Art. 7 DS-GVO).
- besondere Sorgfalt zur Sicherstellung der Freiwilligkeit im Beschäftigungskontext (§ 26 Abs. 2 BDSG)
- transparente Information der Betroffenen gemäß Art. 13 DS-GVO.

Empfehlungen

- ✓ Verwenden Sie klare, verständliche Einwilligungstexte.
- ✓ Machen Sie die Teilnahme freiwillig – kein Druck durch Vorgesetzte.
- ✓ Dokumentieren Sie jede Einwilligung digital.
- ✓ Fügen Sie einen leicht zugänglichen „Widerrufen"-Button oder ein Formular hinzu.

Praxisbeispiel

Die Verarbeitung personenbezogener Daten im Projekt „KI-gestütztes Onboarding" stützt sich auf zwei getrennte Einwilligungen.

Für die Erfassung und Aufbereitung des Praxiswissens der erfahrenen Mitarbeitenden ist eine Einwilligung erforderlich, da die Preisgabe von Erfahrungswissen regelmäßig nicht zu den Arbeitsaufgaben laut Arbeitsvertrag gehört und für dessen Durchführung nicht erforderlich ist...

Quelle: PowerPoint

*Rechtlicher Hinweis: Nach EuGH, Urt. 30.03.2023 - C-34/21 - sind weite Teile des § 26 BDSG unanwendbar. Der Beschäftigtendatenschutz bedarf einer Reform und näheren Ausgestaltung. Anwendungshinweis: Orientierung am – nicht zum Gesetz gewordenen - Referentenentwurf der Vorgängerregierung „Entwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt" (Stand 08.10.2024), abrufbar unter https://www.datenschutz-praxis.de/Nwes-20241018/.

Teil 1: DS-GVO / BDSG

...Auch für das KI-gestützte Onboarding neuer Mitarbeitender ist eine Einwilligung erforderlich, soweit das System über das bloße Ergebnis („bestanden / nicht bestanden") hinaus das individuelle Lernverhalten analysiert und Lernfortschrittsprofile zur Erstellung personalisierter Lernpfade erstellt. Diese Analyse ist für die Aufgabenübertragung nicht erforderlich und bedarf daher einer gesonderten Einwilligung.

Beide Einwilligungen werden freiwillig, informiert und widerruflich eingeholt. Ein Widerruf ist jederzeit ohne Nachteile für das Beschäftigungsverhältnis möglich.

4. Transparenz und Betroffenenrechte

Informationspflichten des Verantwortlichen (Art. 13 und 14 DS-GVO)

Die betroffenen Beschäftigten sind über folgende Punkte zu informieren:

- Zweck und Rechtsgrundlage der Verarbeitung
- Kategorien der Daten
- Empfänger
- Speicherdauer
- Rechte (Art. 15–22 DS-GVO)
- Bestehen automatisierter Entscheidungsfindung – einschließlich Profiling (Art. 22 DS-GVO)

Automatisierte Entscheidungen

Beschäftigte haben das Recht, nicht ausschließlich einer automatisierten Entscheidung unterworfen zu werden, die rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt (Art. 22 DS-GVO). KI-Systeme müssen daher menschliche Kontrollmechanismen und ein Letztentscheidungsrecht vorsehen.

Empfehlungen

- ✓ Stellen Sie sicher, dass alle betroffenen Beschäftigten transparent über den Zweck und die Rechtsgrundlage der Datenverarbeitung informiert werden.
- ✓ Geben Sie klare Informationen zu den Datenkategorien, Empfängern und der Speicherdauer.
- ✓ Informieren Sie die Mitarbeiter über ihre Rechte nach Art. 15–22 DS-GVO.
- ✓ Implementieren Sie menschliche Kontrollmechanismen bei automatisierten Entscheidungen, um ein Letztentscheidungsrecht zu gewährleisten.

Praxisbeispiel

Der Arbeitgeber erfüllt seine Informationspflichten, indem er allen betroffenen Mitarbeitenden ein Datenschutz-Merkblatt zur Verfügung stellt. Dieses informiert transparent über die gemeinsamen Verantwortlichen, die Zwecke der Verarbeitung, die Kategorien personenbezogener Daten, die Speicherdauer sowie die Betroffenenrechte.

Darüber hinaus enthält das Merkblatt aussagekräftige Informationen über die Funktionsweise des KI-Systems, insbesondere:

- welche Eingabedaten verwendet werden,
- nach welchen zentralen Bewertungskriterien Lernfortschritte beurteilt werden und
- wie diese Kriterien zueinander gewichtet sind,
- inwieweit Entscheidungen automatisiert vorbereitet werden und welche Folgen sich daraus ergeben können,
- wie ein menschliches Eingreifen in den Entscheidungsprozess vorgesehen ist.

Quelle: PowerPoint

Die Mitarbeitenden werden darüber informiert, dass eine Joint Controller Vereinbarung nach Art. 26 DS-GVO besteht.

Der wesentliche Inhalt dieser Vereinbarung wird ihnen zusammen mit dem Merkblatt zugänglich gemacht.

Zur Wahrnehmung der Betroffenenrechte richtet der Arbeitgeber klare Prozesse ein, über die Auskunfts-, Berichtigungs-, Lösch- und Kontrollrechte effizient geltend gemacht werden können.

5. Mitbestimmung des Betriebsrats

Nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) hat der Betriebsrat ein zwingendes Mitbestimmungsrecht, wenn technische Systeme eingeführt werden, die geeignet sind, Verhalten oder Leistung von Beschäftigten zu überwachen. Dazu zählen auch KI-Systeme, die personenbezogene Daten analysieren und Muster zu Leistung, Verhalten oder Gesundheit erkennen. Zusätzlich hat der Betriebsrat umfassende Unterrichtungs- und Beratungsrechte nach §§ 90, 92 BetrVG.

In der Praxis ist deshalb eine Betriebsvereinbarung erforderlich, bevor ein KI-System eingeführt oder produktiv genutzt werden darf. Diese muss regelmäßig geprüft und ggf. angepasst werden.

Empfehlungen

- ✓ Binden Sie den Betriebsrat frühzeitig und vollständig in die Planung des KI-Systems ein.
- ✓ Stellen Sie alle relevanten Informationen bereit: Datenarten, Funktionsweise, Risiken, Zweck.
- ✓ Erarbeiten Sie gemeinsam eine klare Betriebsvereinbarung zur Nutzung der KI und überprüfen diese in regelmäßigen Abständen.

Praxisbeispiel

Da das KI-Onboarding-System das Lernverhalten und die Leistung neuer Mitarbeitender auswertet, ist der Betriebsrat zu beteiligen. Das Unternehmen legt dem Betriebsrat die Funktionsweise des Systems, die verarbeiteten Daten und die Auswirkungen auf Beschäftigte offen.

Eine Betriebsvereinbarung regelt insbesondere Zweck, Einsatzbereich, Zugriffsbeschränkungen, Transparenz sowie das Recht auf menschliche Kontrolle über KI-gestützte Bewertungen.

6. Besondere Schutzmaßnahmen

Datenschutz-Folgenabschätzung (DSFA)

Eine DSFA ist erforderlich, wenn die geplante Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der Beschäftigten mit sich bringt (Art. 35 DS-GVO). Dies gilt insbesondere bei neuen Technologien wie KI, bei Profiling oder automatisierter Leistungsbewertung sowie bei der Verarbeitung besonderer Kategorien personenbezogener Daten, wie Gesundheitsinformationen.

Die DSFA umfasst eine:

- eine Beschreibung der Verarbeitungsvorgänge
- eine Bewertung der Notwendigkeit
- eine Risikoanalyse sowie
- Maßnahmen zur Risikominimierung.

Teil 1: DS-GVO / BDSG

Technische und organisatorische Maßnahmen (TOMs, Art. 32 DS-GVO)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos sind gemäß Art. 32 DS-GVO angemessene TOMs umzusetzen. Beispiele für TOMs sind:

- Zugriffskontrollen
- Pseudonymisierung
- Verschlüsselung
- Protokollierung
- Schulungen
- Bias-Schutz und Nachvollziehbarkeit der KI.

Quelle: Pixabay

Bestellung eines Datenschutz-beauftragten (Art. 37, 38 DS-GVO)

Ein Datenschutzbeauftragter muss bestellt werden, wenn:

- mindestens 20 Personen automatisiert mit personenbezogenen Daten arbeiten (§ 38 Abs. 1 BDSG) oder
- die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art 37 Abs 1 c) DS-GVO) oder
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (Gesundheits-daten) besteht (Art. 37 Abs. 1 c) DS-GVO)

Teil 1: DS-GVO / BDSG

Empfehlungen

- ✓ Führen Sie eine DSFA durch, wenn Sie ein KI-System einführen und sensitive Daten verarbeiten.
- ✓ Implementieren Sie angemessene TOMs, um die Datenrisiken zu minimieren.
- ✓ Bestellen Sie einen Datenschutzbeauftragten, wenn Sie die gesetzlichen Voraussetzungen erfüllen.
- ✓ Schulen Sie alle betroffenen Mitarbeiter regelmäßig in Datenschutzthemen, insbesondere im Umgang mit KI-Systemen.
- ✓ Dokumentieren Sie alle Maßnahmen.

Praxisbeispiel

Für das KI-gestützte Onboarding wird eine DSFA durchgeführt, da mit der individuellen Lernfortschrittskontrolle eine systematische und umfassende Leistungsbewertung verbunden ist. Als identifizierte Risiken werden insbesondere der Missbrauch von Lernfortschrittsdaten zur Leistungs- oder Verhaltenskontrolle, unbefugter Zugriff, fehlende Transparenz sowie Risiken im Zusammenhang mit der Einbindung externer Dienstleister oder bei Datenübermittlungen ins Ausland bewertet.

Zur Risikominderung wird in der Joint Controller Vereinbarung verbindlich geregelt, dass der Dienstleister keine personenbezogenen oder auf Personen beziehbare Lernfortschrittsdaten an den Arbeitgeber weitergeben darf…

…An den Arbeitgeber wird ausschließlich das abschließende Ergebnis des Onboardings übermittelt. Dadurch wird eine informationelle Gewaltenteilung sichergestellt und eine klare Zweckbindung festgelegt…

…Es werden TOMs umgesetzt, insbesondere:

- Diskriminierungsfreiheit: regelmäßige Überprüfung des KI-Systems auf diskriminierende und unrichtige Ergebnisse,
- Zugriffskontrolle: nur befugte Personen des Dienstleisters (nicht der Arbeitgeber) dürfen auf personenbezogene Onboarding- und Lernfortschrittsdaten zugreifen,
- Verschlüsselung: verschlüsselte Übertragung und Speicherung der Daten,
- Protokollierung: Zugriffe und Änderungen werden dokumentiert.

Der Arbeitgeber erstellt für das Projekt „KI-gestütztes Onboarding“ ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO…

...Darin werden insbesondere die gemeinsamen Verantwortlichen, die Zwecke der Verarbeitung, die Kategorien betroffener Personen und personenbezogener Daten, mögliche Empfänger etwaige Drittlandübermittlungen, Löschfristen sowie die eingesetzten technischen und organisatorischen Maßnahmen dokumentiert. Das Verzeichnis dient als zentrale Grundlage für Transparenz, die Wahrnehmung von Betroffenenrechten sowie für die Durchführung und Aktualisierung der DSFA.

Ergänzend werden interne Schulungen der HR-Abteilung durchgeführt. Ein externer Datenschutzbeauftragter begleitet die Umsetzung und den laufenden Betrieb.

7. Internationale Datenverarbeitung

Internationale Datenverarbeitung bezieht sich auf die Übermittlung personenbezogener Daten aus der EU in Drittländer, d.h. in Länder außerhalb der EU oder des Europäischen Wirtschaftsraums (EWR).

Nach der DS-GVO ist diese Datenübermittlung nur zulässig, wenn ein angemessenes Datenschutzniveau gewährleistet ist (Art. 44 ff. DS-GVO).

Mögliche Instrumente zur Sicherstellung des Datenschutzniveaus:

- **Angemessenheitsbeschluss der EU-Kommission**: Wird von der EU-Kommission erteilt, wenn ein Drittland ein angemessenes Schutzniveau für personenbezogene Daten bietet (z. B. EU-US Data Privacy Framework).
- **Standardvertragsklauseln für die Übermittlung personenbezogener Daten**: Vordefinierte Vertragsklauseln für Unternehmen, um den Schutz personenbezogener Daten in Drittländern sicherzustellen.
- **Binding Corporate Rules:** Intern für multinationale Konzerne entwickelte Regeln, um Daten innerhalb der Unternehmensgruppe international übertragen zu können.

Empfehlungen

- ✓ Speichern Sie Daten möglichst auf Servern in der EU (Achten Sie darauf, dass der Auftragsverarbeitungsvertrag / AVV keine Unterauftragsverarbeitung in Drittländern zulässt).
- ✓ Stellen Sie andernfalls fest, ob ein Angemessenheitsbeschluss der EU-Kommission für das Drittland besteht.
- ✓ Integrieren Sie Standardvertragsklauseln in Verträge mit Drittanbietern und ggf. Binding Corporate Rules.
- ✓ Sensibilisieren Sie Ihre Mitarbeitenden für Anforderungen und Risiken internationaler Datenübertragungen.

Praxisbeispiel

Sofern der externe Dienstleister personenbezogene Daten außerhalb der EU oder des EWR verarbeitet, stellt der Arbeitgeber sicher, dass ein angemessenes Datenschutzniveau besteht. Die Übermittlung erfolgt ausschließlich unter Nutzung geeigneter Garantien, z. B. beim Datentransfer in die USA durch Zertifizierung des Empfängers nach dem EU-US Data Privacy Framework oder durch ergänzende vertragliche Sicherungsmaßnahmen.

Die Mitarbeitenden werden transparent über die internationale Datenverarbeitung informiert, und die Risiken werden im Rahmen der DSFA berücksichtigt.

Teil 1: DS-GVO / BDSG

Die wichtigsten Gesetze und Paragraphen im Überblick

Die Seitenangabe verweist auf die Stelle in diesem Leitfaden, an der auf den Artikel Bezug genommen wird.

Teil 1: DS-GVO / BDSG

Die wichtigsten Gesetze und Paragraphen im Überblick

BDSG

§ 26
Besondere Anforderungen an die Datenverarbeitung im Beschäftigungskontext
(S. 6 f.)

§ 38 Abs. 2
Ernennung eines Datenschutz-beauftragten
(S. 13 ff.)

§ 26 Abs. 2
Einwilligung in die Datenverarbeitung im Beschäftigungskontext
(S. 9 f.)

BetrVG

§ 87 Abs. 1 Nr. 6
Mitbestimmungsrecht Betriebsrat
(S. 11 f.)

§ 90 u. 92
Unterrichtungs- und Beratungsrechte des Betriebsrats
(S. 11 f.)

Die Seitenangabe verweist auf die Stelle in diesem Leitfaden, an der auf den Artikel Bezug genommen wird.

Teil 1: DS-GVO / BDSG

Glossar

Anonymisierung: Veränderung von personenbezogenen Daten, sodass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

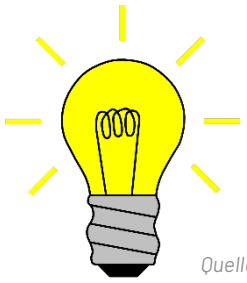
Aufsichtsbehörde: Eine von einem Mitgliedstaat gemäß Art. 51 GS-GVO eingerichtete unabhängige staatliche Stelle.

Auftragsverarbeiter: Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Dritter: Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Einwilligung: Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Gesundheitsdaten: Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (z. B. medizinische Diagnosen und Behandlungen, ärztliche Befunde, Informationen zu Allergien oder Behinderungen, Biomarker wie Blutdruck oder Blutzucker, Krankmeldungen sowie Versichertendaten).



Quelle: Pixabay

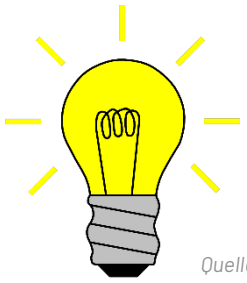
Teil 1: DS-GVO / BDSG

Glossar

Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Zu den besonderen Kategorien personenbezogener Daten zählen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

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

Pseudonymisierung: Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.



Quelle: Pixabay

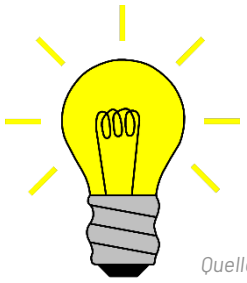
Teil 1: DS-GVO / BDSG

Glossar

Verantwortlicher: Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Verarbeitung: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter 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.

Verletzung des Schutzes personenbezogener Daten: Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.



Quelle: Pixabay

Teil 2: KI-VO

Die KI-VO, auch als „AI Act" bezeichnet, verfolgt das Ziel, die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen KI in der EU zu fördern und gleichzeitig ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte zu gewährleisten.

1. Begriffsbestimmung und Anwendungsbereich

Definition von KI-Systemen

Ein KI-System ist laut Art. 3 Nr. 1 KI-VO ein maschinengestütztes System, das für den autonomen Betrieb ausgelegt ist und sich nach der Betriebsaufnahme anpassen kann. Es verarbeitet Eingaben und erzeugt daraus Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen.

Inkrafttreten und Anwendbarkeit (Art. 113 KI-VO)

Die KI-VO ist am 2. August 2024 in Kraft getreten; der Hauptteil der VO einschließlich der Regelungen für Hochrisikosysteme (Anhang III) gilt ab dem 02.08.2026* mit Ausnahme:

- Kapitel I und II (ab 2. Februar 2025)
- Kapitel III Abschnitt 4, Kapitel V, VII und XII sowie Art. 78 (ab 2. August 2025, Ausnahme Art. 101)
- Art. 6 Abs. 1 (2. August 2027)

Hochrisiko-KI-Systeme, die vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden und nicht wesentlich verändert wurden, unterliegen nicht den neuen Anforderungen (Art. 111 Abs. 2 u. 3 KI-VO).** Hochrisiko-KI-Systeme sind KI-Anwendungen, die potenziell erhebliche Risiken für die Betroffenen darstellen (siehe S. 20).

Empfehlungen

- ✓ Identifizieren Sie, ob Ihre KI nach der Definition überhaupt der KI-Verordnung unterfällt.
- ✓ Berücksichtigen Sie den zeitlichen Anwendungsbereich der einzelnen Abschnitte der KI-VO.
- ✓ Achten Sie bereits jetzt darauf, dass Ihre KI-Systeme der KI-VO entsprechen (Compliance by Design).
- ✓ Bleiben Sie über regulatorische Änderungen informiert. Nutzen Sie kommende harmonisierte Standards und Leitlinien der EU-Kommission (insb. Hochrisiko-KI-Kriterien) und Muster.

Praxisbeispiel

Beim KI-gestützten Onboarding kommen generative Sprach- und Analysemodelle zum Einsatz, die als KI-Systeme im Sinne der KI-VO einzustufen sind...

* Nach dem Vorschlag der EU-Kommission einer Digital-Omnibus-VO vom 19.11.2025 könnte die Frist 02.08.2026 bis längstens 02.12.2027 verlängert werden (weil harmonisierte EU-Standards fehlen und Unternehmen realistische Umsetzungsfristen gegeben werden sollen). Dies wäre insbesondere für den HR- und den Bildungsbereich relevant.
** Nach derzeit herrschender Ansicht gilt die Befreiung nach Art. 111 Abs, 2 KI-VO „werkstückbezogen" / einzel-systembezogen, nicht produktreihenbezogen.

Teil 2: KI-VO

... Die Anwendbarkeit der KI-VO hängt vom Zeitpunkt der Inbetriebnahme ab. Wird das System vor dem 02.08.2026 (*02.12.2027?*) in Betrieb genommen und hat danach keine wesentlichen Änderungen erfahren, muss das Unternehmen die Anforderungen der KI-VO nicht erfüllen.

2. Risikoklassifizierung von KI-Systemen - Hochrisiko-KI-Systeme

Mit der KI-VO wird ein risikobasierter Ansatz verfolgt (siehe Abbildung). Je höher das mit dem KI-System verbundene Risiko ist, umso umfangreicher ist der Pflichtenkatalog, den die Unternehmen erfüllen müssen.

KI-Systeme gelten als hochriskant, wenn sie sich potenziell auf die Sicherheit von Menschen oder ihrer Grundrechte auswirken können. Im Bereich Human Resources zählen dazu:

- Systeme im Bereich der allgemeinen und beruflichen Bildung, insb. zur Bewertung von Lernergebnissen, die den Lernprozess in Bildungseinrichtungen steuern (Anhang III, Ziff. 3 KI-VO).
- Systeme im Bereich Beschäftigung/Personalmanagement, insb. zur Auswahl/Einstellung oder zur Beobachtung und Bewertung von Arbeitsleistungen (Anhang III, Ziff. 4 KI-VO).

Hochrisiko-KI-Systeme sind nicht unzulässig, jedoch unterliegen sie erhöhten regulatorischen Anforderungen, die vom Anbieter zu berücksichtigen sind.

In Anlehnung an Europäische Kommission (2025)

Empfehlungen

- ✓ Identifizieren Sie, ob Ihr System als hochriskant gilt.
- ✓ Machen Sie sich mit den besonderen Anforderungen eines Hochrisiko-Systems vertraut.

Praxisbeispiel

Das im Projekt „KI-gestütztes Onboarding“ eingesetzte KI-System ist als Hochrisiko-KI-System einzustufen.

Europäische Kommission (2025). KI-Gesetz. Abgerufen am 01.12.2025 von https://digital-strategy.ec.europa.eu/de/node/9745/printable/pdf

Teil 2: KI-VO

...Maßgeblich ist dabei nicht die technische Ausgestaltung, sondern wofür das System eingesetzt wird.

Das System wird genutzt, um neue Mitarbeitende digital einzuarbeiten. Es stellt Lerninhalte bereit, wertet Lernfortschritte aus und passt den weiteren Lernverlauf individuell an. Damit bewertet die KI Lernergebnisse und steuert den Lernprozess. Soweit dies im Rahmen eines strukturierten Bildungsangebotes erfolgt, fällt der Einsatz unter Hochrisiko-KI-Systeme im Bereich der allgemeinen und beruflichen Bildung.

Zugleich hat das Ergebnis des KI-gestützten Onboardings Auswirkungen auf den beruflichen Einsatz der neuen Mitarbeitenden. Die automatisierte Lernfortschrittskontrolle liefert eine Bewertung der individuellen Leistung und kann beeinflussen, welche Aufgaben dem Beschäftigten im Unternehmen zugewiesen werden. Dadurch ist das System auch dem Bereich Beschäftigung und Personalmanagement zuzuordnen.

Da das KI-gestützte Onboarding eine Analyse des individuellen Lernverhaltens beinhaltet, liegt ein Profiling vor. Eine Ausnahme von der Hochrisiko-Einstufung scheidet damit aus.

Im Ergebnis ist das eingesetzte KI-System aufgrund seiner Funktion sowohl im Bildungs- als auch im Beschäftigungskontext als Hochrisiko-KI-System einzuordnen. Entsprechend sind die Anforderungen der KI-VO zu beachten.

3. Rollen und Verantwortlichkeiten

Eine klare Rollenbestimmung ist fundamental!

In der KI-VO werden verschiedene Akteure definiert, die jeweils spezifische abgestufte Pflichten haben. Im Zentrum stehen die Rollen des „Anbieters“ (Art. 3 Nr. 3 KI-VO) und des „Betreibers“ (Art. 3 Nr. 4 KI-VO) von KI-Systemen.

Quelle: PowerPoint

Teil 2: KI-VO

Anbieter

...ist eine Person oder ein Unternehmen, das ein KI-System entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Marke in Verkehr bringt bzw. in Betrieb nimmt.

...müssen die Anforderungen der KI-VO von Anfang an in den Entwicklungsprozess integrieren um sicherzustellen, dass die Systeme den gesetzlichen Vorgaben entsprechen.

Betreiber

...ist eine Person oder ein Unternehmen, das ein KI-System in eigener Verantwortung verwendet, es sei denn, dies erfolgt ausschließlich für private Zwecke.

Unternehmen im Bereich HR und Bildung werden selten selbst KI entwickeln. Wird ihnen die KI als AI as a Service (KI-aaS), Infrastructure as a Service (IaaS) oder über Platform as a Service (PaaS) zur Nutzung überlassen, erfolgt der Einsatz eigenverantwortlich und ist das Unternehmen Betreiber des KI-Systems. Wird hingegen der gesamte digitale Prozess auf einen externen Dienstleister ausgelagert - Business Process as a Service (BPaaS) -, nutzt das Unternehmen nur die Ergebnisse dieses Prozesses, ist es nicht Betreiber und unterliegt damit keinen Pflichten nach der KI-VO (*Ansicht des Bearbeiters).*

Risikofalle! Ein zusätzliches Risiko besteht für Betreiber, die ein KI-System mit allgemeinem Verwendungszweck so verändern und einsetzen, dass das KI-System hiernach als Hochrisiko-KI-System zu klassifizieren ist *(z. B. Nutzungsbedingungen OpenAI: GPT nicht für Bildungs- oder Beschäftigungsentscheidungen!)* Der Betreiber wird zum Anbieter und hat sämtliche Anbieter Pflichten nach der KI-VO zu erfüllen, Art. 21 Abs. 1c KI-VO.

Empfehlungen

✓ Verstehen Sie die mit der Rolle des Betreibers verbundenen Pflichten.

Teil 2: KI-VO

- ✓ Wählen Sie Anbieter, die bei der Entwicklung ihrer KI-Systeme alle gesetzliche Anforderungen der KI-VO beachtet haben (Compliance by Design).
- ✓ Führen Sie als Betreiber interne Audits durch, um die Einhaltung der gesetzlichen Vorgaben sicherzustellen.

Praxisbeispiel

Das Projekt „KI-gestütztes Onboarding" wird nach dem Modell Business Process as a Service (BPaaS) ausgestaltet.

Der externe Dienstleister setzt das KI-System eigenständig ein und führt sowohl die Wissensaufbereitung als auch das KI-gestützte Onboarding durch. Der Arbeitgeber nutzt ausschließlich die Endergebnisse und ist nicht Betreiber des KI-Systems im Sinne der KI-VO.

Der Dienstleister ist Betreiber des KI-Systems und unterliegt den Betreiberpflichten der KI-VO. Verändert der Dienstleister die Zweckbestimmung eines KI-Systems mit allgemeinem Verwendungszweck so, dass es als Hochrisiko-KI-System einzustufen ist, wird er gemäß Art. 25 Abs. 1 c) KI-VO zum Anbieter und hat sämtliche Anbieterpflichten zu erfüllen.

4. Pflichten des Anbieters eines Hochrisiko-KI-Systems

Die EU-Kommission hat am 19.11.2025 angekündigt, den Unternehmen noch Instrumente für die praktische Umsetzung in die Hand geben zu wollen. Ein sehr dynamischer Prozess ist zu erwarten. Für die praktische Umsetzung ist daher zu empfehlen, sich an Standards, Leitlinien und Mustern der EU-Kommission, Behörden und Branchenverbänden zu orientieren.

Pflicht	Rechtsgrundlage
Risikobewertung und Risikominderung (einschl. vernünftigerweise vorhersehbarer Fehlanwendungen)	Art. 9 KI-VO
Qualität der Trainingsdaten	Art. 10 KI-VO
Systemdokumen-tation	Art. 11 KI-VO
Protokollierung	Art. 12 KI-VO

Pflicht	Rechtsgrundlage
Betriebsanleitung für Betreiber	Art. 13 KI-VO
Menschliche Aufsicht	Art. 14 KI-VO
Robustheit, Cybersicherheit, Genauigkeit	Art. 105 KI-VO
Konformitätsbewertung und -erklärung	Art. 43, 47 KI-VO
CE-Kennzeichnung	Art. 48 KI-VO
Registrierung in EU-Datenbank	Art. 49 Abs. 1 KI-VO
Transparenzpflicht	Art. 50 KI-VO
Marktbeobachtung nach Inverkehrbringen	Art. 72 KI-VO

Empfehlungen

- ✓ Stellen Sie sicher, dass der Anbieter alle erforderlichen Pflichten erfüllt hat, bevor Sie das System in Betrieb nehmen.
- ✓ Vergewissern Sie sich, dass die vom Anbieter gelieferten Daten und Algorithmen qualitativ hochwertig und nachvollziehbar sind.
- ✓ Richten Sie Prozesse ein, um das System kontinuierlich zu überwachen und menschliche Aufsicht sicherzustellen.

Praxisbeispiel

Der Anbieter des KI-Onboarding-Systems führt eine umfassende Risikobewertung durch, stellt die Qualität der Trainingsdaten sicher und dokumentiert Aufbau und Funktionsweise des Systems.

Er sorgt für Protokollierung, stellt eine Betriebsanleitung bereit und implementiert menschliche Aufsicht. Nach erfolgreicher Konformitätsbewertung erhält das System eine CE-Kennzeichnung und wird in der EU-Datenbank registriert. Die Marktbeobachtung wird fortlaufend durchgeführt.

5. Pflichten des Betreibers eines Hochrisiko-KI-Systems

Pflicht	Rechtsgrundlage
Einsatz gemäß Betriebsanleitung	Art. 26 Abs. 1, 5 KI-VO
Einsatz qualifizierten Personals	Art. 26 Abs. 2 KI-VO

Teil 2: KI-VO

Pflicht	Rechtsgrundlage
Aufbewahrung von Protokollen (mind. 6 Monate)	Art. 26 Abs. 6 KI-VO
Information der Arbeitnehmervertretung	Art. 26 Abs. 6 KI-VO
Information betroffener Personen	Art. 26 Abs. 11 KI-VO
Transparenzpflicht	Art. 50 Abs. 1 KI-VO
Kennzeichnung KI-generierter Inhalte	Art. 50 Abs. 2 KI-VO

Praxisbeispiel

Das Unternehmen stellt sicher, dass das KI-Onboarding-System ausschließlich gemäß der Betriebsanleitung eingesetzt wird.

Qualifiziertes Personal betreut das System, und alle Nutzungs- und Wartungsprotokolle werden mindestens sechs Monate aufbewahrt.

Betriebsrat und neue Mitarbeitende werden über den KI-Einsatz informiert.

Alle durch das System erzeugten Inhalte, etwa Lernempfehlungen oder Auswertungen, werden als KI-generiert gekennzeichnet.

Empfehlungen

- ✓ Nutzen Sie das KI-System stets gemäß der vom Anbieter bereitgestellten Betriebsanleitung.
- ✓ Stellen Sie sicher, dass geschulte Mitarbeiter mit dem System arbeiten.
- ✓ Speichern Sie alle relevanten Protokolle mindestens sechs Monate zur Sicherstellung der Nachvollziehbarkeit.
- ✓ Informieren Sie Arbeitnehmervertretungen und Mitarbeitende über den KI-Einsatz und kennzeichnen Sie KI-generierte Inhalte klar.

Quelle: Pixabay

Teil 2: KI-VO

6. Schnittstelle zur DS-GVO

KI-VO

...z. B. bedingt der Einsatz von Hochrisiko-KI-Systemen eine regelmäßige DSFA gemäß Art. 35 DS-GVO.

DS-GVO

Quelle: Pixabay

Teil 2: KI-VO

Die wichtigsten Artikel der KI-VO im Überblick

Art. 3 Nr. 1
Definition von KI-Systemen
(S. 22 f.)

Art. 3 Nr. 4
Definition Betreiber
(S. 24 f.)

Art. 111 & 113
Inkrafttreten und Anwendbarkeit
(S. 22 f.)

Art. 3 Nr. 3
Definition Anbieter
(S. 24 f.)

Art. 6 ff.
Einstufung und Anforderungen Hochrisiko-KI-Systeme
(S. 23 f.)

Art. 9; 10; 11; 12; 13; 14; 15; 43; 47; 48; 49 Abs. 1; 50 & 72
Pflichten des Anbieters
(S. 26 f.)

Art. 26 Abs. 1, 2, 5, 6, 7, 11 & Art. 50
Pflichten des Betreibers
(S. 27 f.)

Die Seitenangabe verweist auf die Stelle in diesem Leitfaden, an der auf den Artikel Bezug genommen wird.

Teil 2: KI-VO

Glossar

Anbieter: Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.

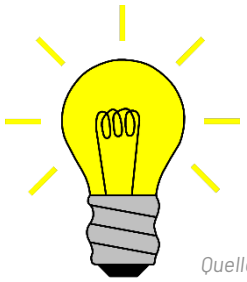
Bereitstellung auf dem Markt: Die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit.

Betreiber: Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.

Betriebsanleitungen: Die Informationen, die der Anbieter bereitstellt, um den Betreiber insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI-Systems zu informieren.

CE-Kennzeichnung: Eine Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System die Anforderungen erfüllt, die in Kapitel III Abschnitt 2 KI-VO und in anderen anwendbaren Harmonisierungsrechtsvorschriften, die die Anbringung dieser Kennzeichnung vorsehen, festgelegt sind;

Eingabedaten: Die in ein KI-System eingespeist oder von diesem direkt erfassten Daten, auf deren Grundlage das System eine Ausgabe hervorbringt.



Quelle: Pixabay

Teil 2: KI-VO

Glossar

Hochrisiko-KI-Systeme: Einstufung nach Art. 6 KI-VO, hier relevant i. V. m. Anhang III:

Ziff. 3. Allgemeine und berufliche Bildung

b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern.

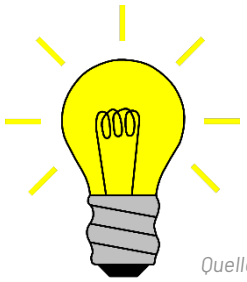
c) KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen.

Ziff. 4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

a) KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten;

b) KI-Systeme, die bestimmungsgemäß für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden soll.

Ausnahme: Abweichend hiervon gilt ein in Anhang III KI-VO genanntes KI-System gemäß Art. 6 Abs. 3 KI-VO nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst; und wenn das KI-System dazu bestimmt ist ...



Quelle: Pixabay

Glossar

... Fortsetzung

- eine eng gefasste Verfahrensaufgabe durchzuführen;
- das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern;
- Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu gedacht, die zuvor abgeschlossene menschliche Bewertung ohne eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen; oder
- eine vorbereitende Aufgabe für eine Bewertung durchzuführen, die für die Zwecke der in Anhang III KI-VO aufgeführten Anwendungsfälle relevant ist.

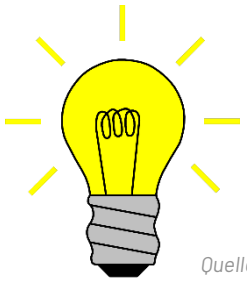
Rückausnahme: Ungeachtet dessen gilt ein in Anhang III aufgeführtes KI-System immer dann als hochriskant , wenn es ein Profiling natürlicher Personen vornimmt.

Inbetriebnahme: Die Bereitstellung eines KI-Systems in der Union zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung.

Informierte Einwilligung. Eine aus freien Stücken erfolgende, spezifische, eindeutige und freiwillige Erklärung der Bereitschaft, an einem bestimmten Test unter Realbedingungen teilzunehmen, durch einen Testteilnehmer, nachdem dieser über alle Aspekte des Tests, die für die Entscheidungsfindung des Testteilnehmers bezüglich der Teilnahme relevant sind, aufgeklärt wurde.

Inverkehrbringen: Die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt.

KI-Kompetenz: Die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden.



Quelle: Pixabay

Teil 2: KI-VO

Glossar

KI-Modell mit allgemeinem Verwendungszweck: Ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden;

KI-System: Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

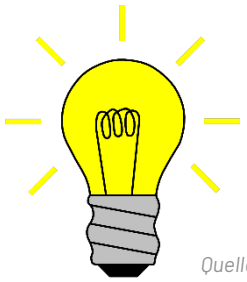
KI-System mit allgemeinem Verwendungszweck. Ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen.

Konformitätsbewertung: Ein Verfahren mit dem bewertet wird, ob die in Kapitel III Abschnitt 2 KI-VO festgelegten Anforderungen an ein Hochrisiko-KI-System erfüllt wurden.

Risiko: Die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens.

System zur Beobachtung nach dem Inverkehrbringen: Alle Tätigkeiten, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Erfahrungen mit der Verwendung der von ihnen in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmaßnahmen zu ergreifen sind.

Trainingsdaten: Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden.



Quelle: Pixabay

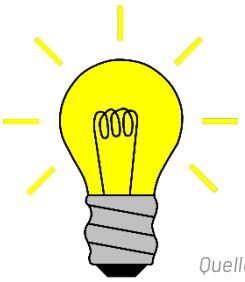
Teil 2: KI-VO

Glossar

Vernünftigerweise vorhersehbare Fehlanwendung: Die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen, auch anderen KI-Systemen, ergeben kann.

Wesentliche Veränderung: Eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde.

Zweckbestimmung: Die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation.



Quelle: Pixabay

Fazit

Die Nutzung von KI-Systemen zur Analyse von Beschäftigtendaten ist datenschutzrechtlich möglich, aber anspruchsvoll. Unternehmen und Dienstleister müssen ihre Rollen klar definieren, die Einhaltung der DS-GVO und des BDSG sicherstellen sowie die Rechte der Beschäftigten wahren. Die Einbindung des Betriebsrats und die transparente Kommunikation sind dabei ebenso essenziell wie technische Schutzmaßnahmen und rechtliche Dokumentation.

Die KI-VO etabliert ein Regelwerk für die Entwicklung und den Einsatz von künstlicher Intelligenz. Unternehmen, die KI-Systeme als Betreiber verwenden, müssen sich ihrer Rolle bewusst sein und die regulatorischen Anforderungen – insbesondere bei Hochrisiko-Anwendungen - konsequent umsetzen. Anbieter wiederum tragen die Verantwortung für die Konformität der Systeme und schaffen die Grundlage für deren rechtssicheren Einsatz im Unternehmen.