

Kostenlose Vorlage · Stand Oktober 2026

KI-Richtlinie für Unternehmen: Muster und Vorlage zum Download

Eine KI-Richtlinie ist eine interne Regel, die festlegt, welche KI-Tools Mitarbeitende nutzen dürfen, welche Daten sie eingeben dürfen und wer neue Anwendungen freigibt. Ein Gesetz verlangt kein Dokument mit diesem Namen, aber Regeln und Schulungsmaßnahmen sind faktisch Pflicht. Diese Vorlage enthält 17 Abschnitte und fünf Anhänge, die Sie in Word ausfüllen und im Unternehmen einführen können.

Inhalt

KI-Richtlinie [Firmenname]

1. Zweck und Geltungsbereich
 2. Begriffe
 3. Grundsätze
 4. Freigegebene Tools
 5. Datenklassen: Was darf in welches Tool?
 6. Verbotene und eingeschränkte Nutzungen
 7. Prüfen von Ergebnissen
 8. Kennzeichnung und Transparenz
 9. Urheberrecht und Geschäftsgeheimnisse
 10. Datenschutz
 11. Informationssicherheit
 12. KI-Kompetenz und Schulung
 13. Neue Tools und Anwendungsfälle beantragen
 14. Rollen und Verantwortlichkeiten
 15. Betriebsrat
 16. Verstöße und Meldungen
 17. Überprüfung und Inkrafttreten
- Anhang A: Tool-Register (Vorlage)
- Anhang B: Antrag auf Freigabe eines KI-Tools oder Anwendungsfalls
- Anhang C: Schulungsnachweis
- Anhang D: Kurzfassung für alle Mitarbeitenden (eine Seite)
- Anhang E: Bestätigung der Kenntnisnahme

KI-Richtlinie [Firmenname]

Version	[1.0]
Gültig ab	[Datum]
Verantwortlich für dieses Dokument	[Name, Funktion]
Nächste planmäßige Überprüfung	[Datum, spätestens 12 Monate nach Inkrafttreten]
Freigegeben durch	[Name, Geschäftsführung]

Hinweis zur Anpassung: Alle Angaben in eckigen Klammern sind durch Ihre Angaben zu ersetzen oder zu streichen. Die Vorlage ist ein Muster und ersetzt keine Rechtsberatung. Rechtsstand: Oktober 2026. Prüfen Sie den Text vor der Einführung mit Ihrer oder Ihrem Datenschutzbeauftragten und, falls vorhanden, mit dem Betriebsrat.

1. Zweck und Geltungsbereich

1.1 Diese Richtlinie regelt, wie die Mitarbeitenden von [Firmenname] („das Unternehmen“) Systeme der künstlichen Intelligenz nutzen dürfen. Sie soll die Chancen der KI für das Unternehmen nutzbar machen und zugleich Datenschutz, Geschäftsgeheimnisse, Urheberrechte, Informationssicherheit und die Rechte von Kunden und Beschäftigten schützen.

1.2 Sie gilt für alle Beschäftigten, Auszubildenden, Praktikantinnen und Praktikanten, Leiharbeitnehmenden, freien Mitarbeitenden und externen Dienstleister, die im Auftrag des Unternehmens arbeiten (zusammen „Mitarbeitende“), an allen Standorten und in jedem Arbeitsmodell, auch im Homeoffice und mobil.

1.3 Sie gilt für jede berufliche Nutzung von KI-Systemen, unabhängig davon, ob das Tool vom Unternehmen bereitgestellt wird, ob es kostenlos ist oder ob es auf privaten Geräten läuft. Sie gilt auch für KI-Funktionen, die in anderer Software enthalten sind, zum Beispiel in Office-Programmen, im E-Mail-Programm, in Übersetzungs- oder Meeting-Tools.

1.4 Weitergehende Regeln, insbesondere zu Datenschutz, Informationssicherheit und Geheimhaltung, bleiben unberührt. Bei Widersprüchen gilt die strengere Regel.

2. Begriffe

Begriff	Bedeutung in dieser Richtlinie
KI-System	Software, die aus Eingaben selbstständig Ausgaben wie Texte, Bilder, Vorhersagen, Empfehlungen oder Entscheidungen erzeugt.
Generative KI	KI-Systeme, die neue Inhalte wie Texte, Bilder, Audio, Video oder Programmcode erzeugen, zum Beispiel Chatassistenten.
Prompt	Jede Eingabe in ein KI-System: Frage, Anweisung, hochgeladene Datei, eingefügter Text, Bild oder Sprachaufnahme.
Ausgabe	Alles, was das KI-System zurückgibt: Text, Zahlen, Bilder, Code, Zusammenfassungen, Übersetzungen.
Freigegebenes Tool	Ein KI-System, das im Tool-Register (Anhang A) steht. Nur diese Tools dürfen beruflich genutzt werden.

Begriff	Bedeutung in dieser Richtlinie
Firmenkonto	Ein vom Unternehmen eingerichteter Zugang mit Firmen-E-Mail-Adresse oder Single Sign-on. Private Konten sind keine Firmenkonten.
KI-Agent	Ein KI-System, das selbstständig mehrere Schritte ausführt und dabei auf andere Systeme zugreift, zum Beispiel E-Mails liest, Dateien ändert oder Bestellungen anlegt.
Personenbezogene Daten	Alle Angaben, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Nr. 1 DSGVO), auch indirekt, etwa über Kundennummer, Fahrzeugkennzeichen oder Schilderung der Umstände.
Besondere Kategorien	Daten nach Art. 9 DSGVO, zum Beispiel Gesundheitsdaten, Gewerkschaftszugehörigkeit, Religion, biometrische und genetische Daten.
Geschäftsgeheimnis	Informationen, die nicht allgemein bekannt sind, wirtschaftlichen Wert haben und vom Unternehmen geheim gehalten werden, etwa Preiskalkulationen, Konstruktionsdaten, Rezepturen (§ 2 Nr. 1 GeschGehG).

3. Grundsätze

3.1 Der Mensch entscheidet. KI-Systeme liefern Vorschläge und Entwürfe. Entscheidungen, die Kunden, Beschäftigte, Lieferanten oder das Unternehmen wesentlich betreffen, trifft immer ein Mensch, der Inhalt und Folgen verstanden hat.

3.2 Die Verantwortung bleibt bei der Person. Wer eine Ausgabe verwendet, verantwortet sie, als hätte sie die Person selbst geschrieben. „Die KI hat das gesagt“ ist keine Begründung.

3.3 Daten schützen. In ein KI-System kommt nur, was nach Abschnitt 5 für dieses Tool zulässig ist. Im Zweifel wird nachgefragt, bevor eingegeben wird.

3.4 Transparent handeln. Wo KI die Arbeit wesentlich geprägt hat und Dritte sich darauf verlassen, wird das offen gesagt (Abschnitt 8). Niemand gibt KI-Ergebnisse als eigene Recherche, als Messung oder als Aussage einer realen Person aus.

3.5 Fair und diskriminierungsfrei. KI wird nicht so eingesetzt, dass Personen wegen geschützter Merkmale benachteiligt werden (Allgemeines Gleichbehandlungsgesetz).

3.6 Ausprobieren ist erwünscht, im Rahmen dieser Regeln. Das Unternehmen will, dass Mitarbeitende KI sinnvoll nutzen. Neue Ideen werden nach Abschnitt 13 geprüft.

4. Freigegebene Tools

4.1 Beruflich genutzt werden dürfen nur KI-Tools, die im Tool-Register (Anhang A) stehen. Das Register nennt für jedes Tool die zulässigen Zwecke und die höchste zulässige Datenklasse.

4.2 Ein Tool wird nur freigegeben, wenn mindestens folgende Punkte geprüft sind:

- Vertrag für Unternehmen vorhanden (keine Verbraucherversion)
- Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen, sofern personenbezogene Daten verarbeitet werden
- Eingaben und Ausgaben werden nicht zum Training der Modelle des Anbieters verwendet, oder dies lässt sich abschalten und ist abgeschaltet
- Speicherort und Drittlandübermittlung geklärt (EU-Hosting oder wirksame Garantien)
- Anmeldung über Firmenkonto, möglichst mit Single Sign-on und Mehrfaktor-Anmeldung

- Löschfristen für Verläufe und Dateien bekannt und eingestellt
- Verantwortliche Person benannt

4.3 Das Tool-Register führt [Name, Funktion, zum Beispiel KI-Verantwortliche/r]. Es ist für alle Mitarbeitenden im Intranet unter [Ort] einsehbar.

4.4 Beispiele für den Aufbau des Registers stehen in Anhang A. Sie sind Platzhalter und keine Empfehlung für ein bestimmtes Produkt.

5. Datenklassen: Was darf in welches Tool?

5.1 Das Unternehmen unterscheidet fünf Datenklassen. Enthält eine Eingabe Daten mehrerer Klassen, gilt die höchste.

Klasse	Beschreibung	Beispiele aus dem Betrieb
1 Öffentlich	Bereits veröffentlicht oder zur Veröffentlichung bestimmt	Texte der Website, Produktkataloge, Stellenanzeigen, Pressemitteilungen, allgemeine Fachfragen
2 Intern	Nicht öffentlich, aber ohne großen Schaden bei Bekanntwerden	Arbeitsanweisungen, Besprechungsagenden ohne Namen Dritter, interne Rundschreiben, Entwürfe für Produkttexte
3 Vertraulich	Geschäftsgeheimnisse und vertragliche Informationen	Angebote und Preislisten, Konditionen, Verträge, Lieferantenbedingungen, Umsatz- und Kostenzahlen, Projektpläne
4 Personenbezogen	Daten identifizierbarer Personen	Kundenkontakte und Ansprechpartner, Bestellungen mit Namen, Mitarbeiterlisten, Bewerbungen, E-Mail-Verläufe mit Namen, Support-Tickets
5 Streng vertraulich	Besondere Kategorien nach Art. 9 DSGVO, Personalakten und besonders wertvolle Geschäftsgeheimnisse	Krankmeldungen und Gesundheitsdaten, Abmahnungen, Gehaltsabrechnungen, Personalakten, Konstruktionsdaten und Rezepturen des Kernprodukts, Quellcode der Kernsoftware, Unternehmenszahlen vor Veröffentlichung, M&A-Unterlagen

5.2 Auch ohne Namen kann ein Personenbezug bestehen. Die DSK weist darauf hin, dass es meist nicht reicht, Namen und Anschriften zu entfernen, wenn sich die Person aus dem Zusammenhang bestimmen lässt. Wer anonymisiert, prüft deshalb auch Kundennummern, Positionen, Orte, Daten und Besonderheiten des Falls.

5.3 Es gibt drei Arten von Tools:

- Typ A: Nicht freigegebene oder öffentliche Dienste, zum Beispiel kostenlose Chatassistenten, private Konten, Browser-Erweiterungen und Apps ohne Firmenvertrag.
- Typ B: Freigegebene Tools mit Firmenvertrag (Anhang A), die nach Abschnitt 4.2 geprüft sind.
- Typ C: Eigenbetrieb, also KI-Systeme, die das Unternehmen selbst oder in einer eigenen, abgeschotteten Umgebung betreibt, zum Beispiel auf eigenen Servern oder in einem eigenen Cloud-Mandanten.

5.4 Zulässigkeit:

Datenklasse	Typ A (nicht freigegeben)	Typ B (freigegeben)	Typ C (Eigenbetrieb)
1 Öffentlich	Erlaubt, ohne Anmeldung mit Firmenangaben	Erlaubt	Erlaubt
2 Intern	Verboten	Erlaubt	Erlaubt
3 Vertraulich	Verboten	Erlaubt, wenn im Register für Klasse 3 eingetragen	Erlaubt
4 Personenbezogen	Verboten	Nur für im Register eingetragene Zwecke, mit AVV und Prüfung nach Abschnitt 10	Erlaubt für im Register eingetragene Zwecke
5 Streng vertraulich	Verboten	Verboten, außer mit schriftlicher Einzelfreigabe nach Abschnitt 13	Nur mit schriftlicher Einzelfreigabe nach Abschnitt 13

5.5 Praktische Beispiele:

- Ein Angebot an einen Kunden soll formuliert werden. Mit Typ B erlaubt, wenn das Tool Klasse 3 zulässt. Die Preise sind Klasse 3. Mit einem kostenlosen öffentlichen Tool verboten.
- Eine E-Mail eines Kunden mit Namen und Bestellung soll zusammengefasst werden. Klasse 4. Nur in einem Tool, das dafür im Register steht.
- Eine Produktbeschreibung für den Webshop wird überarbeitet. Klasse 1 oder 2. Mit jedem freigegebenen Tool erlaubt.
- Eine Zeichnung oder Stückliste des Kernprodukts soll geprüft werden. Klasse 5. Verboten ohne schriftliche Einzelfreigabe.
- Die Personalleitung möchte ein Arbeitszeugnis formulieren lassen. Klasse 4, mit Leistungsbeurteilung Klasse 5. Nur nach Freigabe und ohne Namen und erkennbare Einzelheiten.
- Eine Krankmeldung, ein Gehaltsnachweis oder eine Abmahnung gehört nie in ein KI-Tool, solange keine Einzelfreigabe vorliegt.

5.6 Zugangsdaten, Passwörter, Schlüssel, interne Systemadressen und Kundenzugänge dürfen in keine Eingabe, auch nicht als Teil von Code oder Konfigurationsdateien.

6. Verbotene und eingeschränkte Nutzungen

6.1 Verboten

Folgende Nutzungen sind im Unternehmen untersagt:

a) Private Konten und nicht freigegebene Tools für berufliche Zwecke mit Daten ab Klasse 2.

b) Entscheidungen mit Rechtswirkung oder ähnlich erheblicher Wirkung für Personen, die allein durch ein KI-System getroffen werden (Art. 22 DSGVO). Das gilt zum Beispiel für Einstellung, Ablehnung von Bewerbungen, Abmahnung, Kündigung, Schichtzuteilung nach persönlichen Merkmalen, Kreditwürdigkeit oder Sperrung von Kundenkonten. Ein Mensch muss die Entscheidung inhaltlich treffen. Die DSK stellt klar, dass eine bloß formale Beteiligung nicht reicht. Wer Vorschläge der KI übernimmt, braucht tatsächlichen Entscheidungsspielraum und Zeit zur Prüfung.

c) Die automatische Auswertung und Aussortierung von Bewerbungen sowie das automatische Versenden von Einladungen oder Absagen. Die DSK nennt genau dieses Beispiel als Verstoß gegen Art. 22 DSGVO. KI-Unterstützung bei Bewerbungen, etwa für Stellenanzeigen oder Terminabstimmung, ist nach Abschnitt 13 zu beantragen.

d) Überwachung von Mitarbeitenden mit KI, etwa Analyse von Stimme, Mimik oder Tastaturverhalten, und die Erkennung von Emotionen am Arbeitsplatz. Die KI-Verordnung verbietet Systeme zur Emotionserkennung am Arbeitsplatz grundsätzlich (Art. 5 Abs. 1 Buchst. f), außer aus medizinischen oder Sicherheitsgründen.

e) Die Verwendung von KI-Systemen, die nach der KI-Verordnung verboten sind. Dazu gehören in einfachen Worten: Systeme, die Menschen unterschwellig oder durch Täuschung manipulieren, Schwächen etwa wegen Alter oder Behinderung ausnutzen, Menschen anhand ihres Sozialverhaltens bewerten und dafür unverhältnismäßig benachteiligen (Social Scoring), Gesichtsdatenbanken durch ungezieltes Auslesen aufbauen, aus biometrischen Daten auf Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, Religion oder sexuelle Orientierung schließen und Emotionen am Arbeitsplatz erkennen. Ab dem 2. Dezember 2026 kommen nach der Verordnung (EU) 2026/1744 Systeme hinzu, die realistische intime Bilder, Videos oder Tonaufnahmen identifizierbarer echter Personen ohne deren ausdrückliche Einwilligung erzeugen, sowie Systeme zur Erzeugung von Darstellungen sexuellen Kindesmissbrauchs.

f) Das Erzeugen oder Verändern von Bildern, Videos oder Tonaufnahmen realer Personen, die echt wirken, ohne deren ausdrückliche Einwilligung. Mit Einwilligung ist es nur erlaubt, wenn der Inhalt als KI-erzeugt gekennzeichnet wird (Abschnitt 8). Dies gilt auch für Stimmklone von Führungskräften, Kunden oder Beschäftigten. Unabhängig von der KI-Verordnung sind das Recht am eigenen Bild und das allgemeine Persönlichkeitsrecht zu beachten.

g) Die Eingabe von Daten der Klasse 5 und das Hochladen vollständiger Verträge, Personalakten oder Quellcodes des Kernprodukts ohne Einzelfreigabe.

h) Das Umgehen von Schutzmechanismen, Zugriffsrechten und technischen Sperren, etwa durch Verschleierung des Kontexts („Jailbreak“), um verbotene Inhalte oder Daten zu erhalten.

i) Das Veröffentlichen ungeprüfter KI-Ausgaben in Außenwirkung (Abschnitt 7).

6.2 Eingeschränkt erlaubt (nur mit Freigabe oder Auflagen)

Nutzung	Auflage
Personenbezogene Auswertungen (zum Beispiel Kundensegmente, Bewertung von Mitarbeitenden)	Freigabe nach Abschnitt 13, Prüfung durch Datenschutz, bei Beschäftigten Einbindung des Betriebsrats
Unterstützung im Bewerbungsprozess	Nur zur Vorbereitung (Anzeigen, Terminabstimmung). Keine automatische Vorauswahl. Freigabe nach Abschnitt 13
Chatbots und Assistenten für Kunden	Kennzeichnung nach Abschnitt 8, Freigabe, Test, Übergabe an Menschen jederzeit möglich
KI-Agenten mit Systemzugriff	Freigabe, eng gefasste Rechte, Protokollierung, Bestätigung durch Menschen vor schreibenden oder unumkehrbaren Aktionen (Abschnitt 11)
Programmcode für produktive Systeme	Prüfung durch eine zweite Person und Sicherheitscheck, keine Zugangsdaten und kein Kernquellcode in Typ-A-Tools
Rechts-, Steuer-, Gesundheits- und Sicherheitsfragen	Nur als Vorbereitung, nie als Auskunft. Prüfung durch Fachleute

Nutzung	Auflage
Übersetzungen und Texte mit vertraglicher Bedeutung	Prüfung durch eine sprachkundige Person oder die Fachabteilung
Aufzeichnung und Transkription von Gesprächen und Meetings	Information der Beteiligten vorab, im Zweifel Einwilligung, Freigabe, kein Einsatz bei Personalgesprächen ohne Einzelfreigabe

7. Prüfen von Ergebnissen

7.1 KI-Ausgaben können falsch, veraltet, erfunden oder verzerrt sein, auch wenn sie überzeugend klingen. Diese Fehler heißen Halluzinationen. Die DSK weist darauf hin, dass Anbieter selbst klarstellen, dass ihre Texte keinen Anspruch auf Richtigkeit haben.

7.2 Jede Person prüft Ausgaben, bevor sie sie verwendet, weiterleitet oder veröffentlicht. Die Prüftiefe richtet sich nach dem Risiko:

Art der Ausgabe	Mindestprüfung
Interne Notiz, Brainstorming	Plausibilitätsprüfung
Zusammenfassung eines Dokuments	Stichproben gegen das Original. Zahlen, Namen und Fristen immer prüfen
Zahlen, Berechnungen, Tabellen	Nachrechnen oder mit der Quelle abgleichen, nicht auf KI-Rechnung verlassen
Fachliche Aussagen, Quellen, Zitate	Quelle selbst öffnen und lesen. Nicht auffindbare Quellen gelten als erfunden
Rechtstexte, Verträge, Datenschutz, Steuern	Nur als Entwurf. Prüfung durch Rechts- oder Fachabteilung oder externe Beratung
Technische Angaben, Normen, Sicherheit	Prüfung durch fachlich Verantwortliche. Keine Freigabe allein auf KI-Basis
Programmcode	Lesen, testen, Sicherheit prüfen. Keine ungeprüfte Übernahme in produktive Systeme
Texte an Kunden, Lieferanten, Behörden	Vollständig lesen, Ton und Inhalt prüfen, Name und Zusagen kontrollieren
Texte über Personen	Auf Richtigkeit und Diskriminierung prüfen, bevor sie weiterverwendet werden

7.3 Zusagen, Preise, Fristen, Garantien und rechtliche Aussagen, die ein KI-Tool vorschlägt, werden nur nach persönlicher Prüfung übernommen.

7.4 Wer Fehler in einer Ausgabe bemerkt, die schon weitergegeben wurde, meldet das nach Abschnitt 16. Das ist erwünscht und hat keine Nachteile.

8. Kennzeichnung und Transparenz

8.1 Rechtlicher Hintergrund (Stand Oktober 2026): Artikel 50 der KI-Verordnung gilt seit dem 2. August 2026. Er verpflichtet vor allem die Anbieter von KI-Systemen, aber auch Unternehmen, die KI einsetzen („Betreiber“), etwa bei Deepfakes und bei Texten zu Themen von öffentlichem Interesse (Art. 50 Abs. 4). Für Anbieter generativer Systeme, die schon vor dem 2. August 2026 auf dem Markt waren, gilt für die maschinenlesbare Kennzeichnung der Ausgaben (Art. 50 Abs. 2) eine Übergangsfrist bis zum 2. Dezember 2026. Die Hinweispflicht bei der Interaktion mit KI (Art. 50 Abs. 1) und die Pflichten der

Betreiber bei Deepfakes sind davon nicht betroffen. Ob Ihr Unternehmen bei einem eigenen Chatbot als Anbieter oder als Betreiber gilt, hängt vom Einzelfall ab. Wer ein System unter eigenem Namen anbietet, gilt häufig als Anbieter. Im Zweifel holen Sie fachlichen Rat ein.

8.2 Chatbots und Assistenten für Kunden. Wer mit einem KI-System spricht, wird zu Beginn des Kontakts klar darauf hingewiesen, dass es sich um KI handelt, es sei denn, das ist aus den Umständen offensichtlich. Der Hinweis lautet zum Beispiel: „Sie chatten mit einem KI-Assistenten von [Firmenname]. Auf Wunsch übergeben wir an einen Menschen.“ Dasselbe gilt für Telefonassistenten.

8.3 Deepfakes. Bilder, Videos und Audioaufnahmen, die mit KI erzeugt oder verändert wurden und reale Personen, Orte, Gegenstände oder Ereignisse so darstellen, dass sie echt wirken, werden als KI-erzeugt gekennzeichnet. Das gilt auch für Stimmen. Bei offensichtlich künstlerischen, satirischen oder fiktionalen Werken genügt ein Hinweis in geeigneter Form.

8.4 Texte zu Themen von öffentlichem Interesse. Texte, die zur Information der Öffentlichkeit zu Themen von öffentlichem Interesse veröffentlicht werden, müssen als KI-erzeugt gekennzeichnet werden, außer sie wurden von einem Menschen geprüft oder redaktionell kontrolliert und eine Person trägt dafür die redaktionelle Verantwortung. Im Unternehmen gilt: Jeder veröffentlichte Text hat eine namentlich verantwortliche Person, die ihn geprüft hat. Marketingtexte, Produktbeschreibungen und Newsletter sind in der Regel keine Texte dieser Art, werden aber ebenfalls von der verantwortlichen Person geprüft.

8.5 Emotionserkennung und biometrische Kategorisierung. Sie sind im Unternehmen nach Abschnitt 6 verboten. Sollte ein Ausnahmefall (zum Beispiel aus Sicherheitsgründen) freigegeben werden, sind die betroffenen Personen vorab über den Betrieb des Systems zu informieren.

8.6 Intern gilt: Wenn eine Ausgabe wesentlich von KI stammt und andere sich darauf verlassen (Analysen, Berichte, Protokolle, Code), wird dies kurz vermerkt, etwa mit „Entwurf mit [Tool] erstellt, geprüft von [Name]“.

8.7 Kein Hinweis ist nötig für KI-Hilfen mit untergeordneter Bedeutung, zum Beispiel Rechtschreibprüfung, Formulierungsvorschläge, Übersetzungshilfen und Gliederungen, deren Inhalt die Person selbst geprüft und verantwortet.

8.8 Betroffene Personen, deren Daten von KI verarbeitet werden, werden über die Datenschutzhinweise des Unternehmens informiert (Abschnitt 10).

9. Urheberrecht und Geschäftsgeheimnisse

9.1 Eingaben. Fremde urheberrechtlich geschützte Werke (Texte, Bilder, Software, Studien, Handbücher von Herstellern) werden nur eingegeben, wenn das Unternehmen sie nutzen darf und die Nutzungsbedingungen des Tools das zulassen. Vertrauliche Dokumente von Kunden und Lieferanten werden nur eingegeben, wenn Vertrag, Geheimhaltungsvereinbarung und Tool dies zulassen. Im Zweifel fragen Mitarbeitende vorher bei [Rolle].

9.2 Ausgaben. Urheberrechtsschutz nach § 2 Abs. 2 UrhG besteht nur für persönliche geistige Schöpfungen. Ausgaben, die ohne wesentliche eigene gestalterische Leistung einer Person entstehen, sind daher möglicherweise nicht geschützt. Das Unternehmen kann sie dann unter Umständen nicht gegen Nachahmung verteidigen. Für Werke, bei denen Schutz wichtig ist (Logo, Markenauftritt, Kernsoftware, Handbuch), wird KI nur als Hilfe genutzt und die eigene gestalterische Leistung dokumentiert.

9.3 Rechte Dritter. KI-Ausgaben können Inhalte enthalten, die Rechte Dritter verletzen, zum Beispiel Bilder, Stile, Texte oder Code mit Lizenzbindung. Vor einer Veröffentlichung prüfen Mitarbeitende deshalb bei Bildern, Logos, längeren Textpassagen und Programmcode auf

mögliche Verletzungen. Bei Auffälligkeiten wird [Rolle] gefragt. Die Nutzungsbedingungen des Tools (zum Beispiel zu Freistellungen des Anbieters) stehen im Tool-Register.

9.4 Geschäftsgeheimnisse. Informationen sind nur dann als Geschäftsgeheimnis geschützt, wenn das Unternehmen angemessene Geheimhaltungsmaßnahmen getroffen hat (§ 2 Nr. 1 GeschGehG). Diese Richtlinie ist eine solche Maßnahme. Mitarbeitende geben Geschäftsgeheimnisse (Klasse 3 und 5) nur in Tools ein, die dafür im Register stehen.

9.5 Kundeninformationen unterliegen oft vertraglichen Geheimhaltungspflichten. Diese gehen dieser Richtlinie vor, wenn sie strenger sind. Das gilt auch für Vorgaben von Auftraggebern, die den Einsatz von KI bei ihren Daten einschränken oder ausschließen.

9.6 Exportkontrolle. Für Technologie, die der Exportkontrolle unterliegt (zum Beispiel bestimmte Konstruktionsdaten und Software mit doppeltem Verwendungszweck), kann schon die elektronische Übermittlung an Server außerhalb der EU oder die Bereitstellung für Personen außerhalb der EU eine Ausfuhr sein (Art. 2 Nr. 2 Dual-Use-Verordnung (EU) 2021/821). Solche Daten gehören nicht in KI-Tools, bevor [Exportkontrollbeauftragte/r oder Rolle] geprüft hat, ob und unter welchen Bedingungen das zulässig ist. Das gilt auch für Tools mit EU-Hosting, wenn Anbieter oder Support von außerhalb der EU auf die Daten zugreifen können.

10. Datenschutz

10.1 Grundsatz. Personenbezogene Daten dürfen nur in KI-Tools eingegeben werden, wenn dafür eine Rechtsgrundlage besteht (Art. 6 DSGVO), der Zweck festgelegt ist, nur die nötigen Daten verwendet werden (Datenminimierung, Art. 5 DSGVO) und die betroffenen Personen informiert sind. Die DSK betont, dass für die Eingabe und gegebenenfalls die Übermittlung an den KI-Anbieter eine Rechtsgrundlage vorliegen muss.

10.2 Auftragsverarbeitung. Verarbeitet ein Anbieter personenbezogene Daten im Auftrag des Unternehmens, muss vor der ersten Nutzung ein Vertrag nach Art. 28 DSGVO abgeschlossen sein. Ohne diesen Vertrag dürfen keine Daten der Klasse 4 oder 5 in das Tool.

10.3 Training und Verlauf. Für jedes freigegebene Tool ist einzustellen, dass Eingaben und Ausgaben nicht zum Training der Modelle verwendet werden, soweit das möglich ist. Der Speicherverlauf wird nach Möglichkeit abgeschaltet oder auf die kürzeste sinnvolle Dauer begrenzt. Die DSK empfiehlt, Trainingsnutzung und Eingabehistorie bei Firmenkonten von vornherein abzuschalten. [Verantwortliche Person] prüft die Einstellungen bei Einführung und danach bei jeder Änderung der Anbieterbedingungen.

10.4 Löschrufen. Verläufe, hochgeladene Dateien und Ausgaben mit personenbezogenen Daten werden nach [Zahl] Tagen gelöscht, spätestens wenn der Zweck entfällt. Ergebnisse, die als Geschäftsunterlagen aufzubewahren sind, werden in den dafür vorgesehenen Systemen abgelegt, nicht im KI-Tool.

10.5 Datenschutz-Folgenabschätzung. Vor Anwendungen, die voraussichtlich ein hohes Risiko für Betroffene bergen, ist eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Das ist insbesondere der Fall bei umfangreicher Verarbeitung von Daten der Klasse 5, bei systematischer Bewertung von Personen, bei Überwachung von Beschäftigten und bei der Verarbeitung neuer Technik im großen Umfang. Die DSK hält eine Folgenabschätzung bei KI-Anwendungen für vielfach erforderlich. Die oder der Datenschutzbeauftragte entscheidet im Freigabeverfahren, ob sie erforderlich ist. Das Verzeichnis von Verarbeitungstätigkeiten wird ergänzt.

10.6 Betroffenenrechte. Anfragen von Betroffenen zu Auskunft, Berichtigung oder Löschung, die KI-Anwendungen betreffen, werden unverzüglich an [Datenschutzbeauftragte/r] weitergegeben. Der Datenschutzhinweis des Unternehmens nennt, wo KI-Tools personenbezogene Daten verarbeiten.

10.7 Besondere Kategorien (Art. 9 DSGVO) dürfen nur mit Einzelfreigabe und nur, wenn eine Ausnahme nach Art. 9 Abs. 2 DSGVO besteht, in ein KI-System gelangen.

10.8 Ausgaben mit Personenbezug. Auch wenn eine Eingabe keine personenbezogenen Daten enthält, kann die Ausgabe welche enthalten, zum Beispiel bei der Frage nach Informationen zu einer bestimmten Person. Solche Anfragen sind nur zulässig, wenn der Zweck rechtmäßig ist. Ergebnisse über Personen werden vor der Weiterverwendung auf Richtigkeit geprüft.

10.9 Automatisierte Einzelentscheidungen sind nach Abschnitt 6 verboten (Art. 22 DSGVO).

11. Informationssicherheit

11.1 Firmenkonten. KI-Tools werden nur mit Firmenkonten genutzt, nicht mit privaten Konten oder privaten E-Mail-Adressen. Wo möglich wird die Anmeldung über Single Sign-on mit Mehrfaktor-Authentifizierung angebunden. Konten tragen nach Möglichkeit keine Klarnamen in öffentlich sichtbaren Bereichen. Die DSK rät, Geräte und Accounts für die berufliche Nutzung bereitzustellen, damit keine Profile über Beschäftigte bei den Anbietern entstehen. Bestehende private Konten. Wer bisher mit einem privaten Konto beruflich gearbeitet hat, nutzt es ab dem Inkrafttreten nicht mehr dafür, meldet dies bei [Stelle] und löscht Verläufe mit Firmeninhalten, soweit möglich. Wird ein Firmenkonto beendet, weil Mitarbeitende ausscheiden, sperrt [IT] den Zugang und sichert oder löscht die Inhalte nach Abschnitt 10.4.

11.2 Zugriffsrechte. Mitarbeitende erhalten nur Zugriff auf Tools und Datenquellen, die sie für ihre Aufgabe brauchen. KI-Assistenten, die mit Postfach, Dokumentenablage oder Wissensdatenbank verbunden sind, sehen nur das, was die Person selbst sehen darf. [IT] prüft Berechtigungen, bevor ein Assistent an Firmendaten angebunden wird. Das gilt besonders für Assistenten in Microsoft 365 (Copilot): Sie greifen auf alles zu, was die Person im Mandanten lesen darf. Zu weit gefasste Freigaben in SharePoint, Teams oder OneDrive werden deshalb vor dem Einsatz bereinigt, und Dokumente der Klassen 4 und 5 werden entsprechend geschützt (zum Beispiel durch Vertraulichkeitsbezeichnungen).

11.3 Prompt Injection. KI-Systeme können durch versteckte Anweisungen in Dokumenten, E-Mails, Webseiten oder Dateien manipuliert werden. Mitarbeitende laden keine Dokumente aus unbekannten Quellen in Assistenten mit Zugriff auf Firmendaten und folgen keinen Anweisungen, die ein Tool aus fremden Inhalten übernimmt. Ungewöhnliches Verhalten eines Tools wird nach Abschnitt 16 gemeldet. Hinweise zu Schutzmaßnahmen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI).

11.4 KI-Agenten mit Systemzugriff. Agenten dürfen nur eingesetzt werden, wenn sie nach Abschnitt 13 freigegeben sind. Es gilt:

- Der Agent erhält ein eigenes Dienstkonto mit den geringsten nötigen Rechten, nie die Rechte einer Person mit Administratorzugang.
- Lesen und Schreiben sind getrennt. Schreibende, löschende, zahlungsrelevante oder nach außen sichtbare Aktionen (E-Mail-Versand, Bestellungen, Buchungen, Preisänderungen) brauchen die Bestätigung eines Menschen, bis die Freigabe ausdrücklich etwas anderes festlegt.
- Alle Aktionen werden protokolliert. Das Protokoll wird mindestens [Zahl] Monate aufbewahrt.
- Es gibt einen Not-Aus und eine verantwortliche Person.
- Kosten und Aufrufmengen sind begrenzt.

11.5 Plugins, Erweiterungen und Verbindungen. Browser-Erweiterungen, Plugins, Konnektoren und selbst gebaute Automatisierungen (zum Beispiel mit n8n oder Make) werden wie eigene Tools behandelt und brauchen eine Freigabe. Sie dürfen nur mit Zugangsdaten arbeiten, die [IT] verwaltet.

11.6 Eigene Entwicklung. Wer Prompts, Assistenten oder Automatisierungen für andere baut, dokumentiert Zweck, Datenquellen, Rechte und Verantwortliche im Tool-Register.

11.7 Geräte. Auf privaten Geräten werden keine KI-Apps mit Firmendaten genutzt, solange keine Regelung zur privaten Gerätenutzung dies ausdrücklich erlaubt.

11.8 Aufzeichnung und Transkription. Mitarbeitende behandeln Aufzeichnungsfunktionen von Meeting-Assistenten wie andere Aufnahmen: Alle Teilnehmenden, auch externe, werden vor Beginn informiert und stimmen zu. Wer nicht zustimmt, wird nicht aufgezeichnet, oder die Funktion bleibt aus. Heimliche Aufnahmen sind verboten und können nach § 201 StGB strafbar sein. Transkripte enthalten meist personenbezogene Daten und werden nach Abschnitt 10.4 gelöscht. Vertrauliche Gespräche, Personal-, Betriebsrats- und Rechtsgespräche werden nicht aufgezeichnet.

12. KI-Kompetenz und Schulung

12.1 Hintergrund. Nach Artikel 4 der KI-Verordnung ergreift das Unternehmen Maßnahmen, um die KI-Kompetenz seiner Beschäftigten und anderer Personen zu fördern, die in seinem Auftrag KI-Systeme nutzen. Die Maßnahmen berücksichtigen Vorkenntnisse, Aufgaben, Einsatzkontext und die Personen, auf die sich der Einsatz auswirkt. Ein Kompetenzniveau, Zertifikate oder ein KI-Beauftragter sind nicht vorgeschrieben. Die Bundesnetzagentur empfiehlt, die Maßnahmen zu dokumentieren.

12.2 Grundsicherung. Alle Mitarbeitenden, die KI-Tools nutzen, erhalten vor der ersten Nutzung eine Einweisung (mindestens [Dauer, zum Beispiel 60 Minuten]) zu: Funktionsweise und Grenzen, Datenklassen, dieser Richtlinie, Prüfpflicht, Kennzeichnung, Meldeweg. Sie wird einmal jährlich aufgefrischt.

12.3 Vertiefung. Wer KI für besondere Aufgaben nutzt (Personalbereich, Kundenkommunikation, Entwicklung, Einkauf, Agenten und Automatisierungen), erhält eine Zusatzschulung zu den Risiken seines Bereichs.

12.4 Führungskräfte werden zusätzlich zu ihrer Verantwortung für Einhaltung, Vorbildfunktion und Umgang mit Fehlern geschult.

12.5 Dokumentation. Art, Umfang, Inhalt, Datum und teilnehmende Personen jeder Schulung werden im Schulungsnachweis (Anhang C) festgehalten. Verantwortlich ist [Name, Funktion].

12.6 Neue Mitarbeitende erhalten die Einweisung innerhalb von [zwei] Wochen nach Eintritt, in jedem Fall vor der Nutzung von KI-Tools.

12.7 Externe Dienstleister, die für das Unternehmen KI nutzen, werden auf diese Richtlinie verpflichtet.

13. Neue Tools und Anwendungsfälle beantragen

13.1 Wer ein neues KI-Tool oder einen neuen Anwendungsfall nutzen möchte, stellt den Antrag in Anhang B bei [KI-Verantwortliche/r] oder unter [E-Mail/Ticketsystem].

13.2 Ablauf und Fristen:

Schritt	Wer	Frist
Eingangsbestätigung	KI-Verantwortliche/r	[2] Arbeitstage
Erste Einordnung (Risiko niedrig, mittel, hoch)	KI-Verantwortliche/r	[5] Arbeitstage
Prüfung Datenschutz und IT-Sicherheit	Datenschutzbeauftragte/r, IT	[10] Arbeitstage
Information des Betriebsrats, falls betroffen	Geschäftsführung / Personal	vor Einführung, rechtzeitig
Entscheidung und Eintrag ins Register	KI-Verantwortliche/r, bei hohem Risiko Geschäftsführung	[15] Arbeitstage nach vollständigem Antrag

13.3 Risikostufen:

- **Niedrig:** Nur Daten der Klassen 1 und 2, kein Kundenkontakt, kein Systemzugriff.
Entscheidung durch die KI-Verantwortliche oder den KI-Verantwortlichen.
- **Mittel:** Daten der Klasse 3 oder 4, interne Automatisierung, Systemzugriff lesend.
Entscheidung nach Prüfung durch Datenschutz und IT.
- **Hoch:** Daten der Klasse 5, Entscheidungen über Personen, Kundenkontakt in eigenem Namen, schreibender Systemzugriff, Anwendungsfälle im Personalbereich.
Entscheidung durch die Geschäftsführung, Datenschutz-Folgenabschätzung prüfen, Betriebsrat einbinden.

13.4 Ist der Antrag unvollständig, wird nachgefragt. Eine Ablehnung wird begründet.
Erteilte Freigaben können mit Auflagen versehen und widerrufen werden.

13.5 Solange keine Freigabe vorliegt, wird das Tool nicht beruflich genutzt. Die Frist soll sicherstellen, dass niemand aus Ungeduld zu privaten Konten greift. Wird sie überschritten, darf die antragstellende Person bei der Geschäftsführung nachfragen.

13.6 Zu prüfen ist bei jedem Antrag auch, ob das Tool oder der Anwendungsfall in den Bereich Hochrisiko-KI nach der KI-Verordnung fällt, etwa im Personalwesen oder bei Bewertungen von Personen. Für solche Systeme gelten zusätzliche Pflichten, die nach der Verordnung (EU) 2026/1744 für eigenständige Hochrisiko-Systeme (Anhang III, dazu gehört der Bereich Beschäftigung und Personalmanagement) erst ab dem 2. Dezember 2027 anwendbar sind. Das verschiebt den Termin, ändert aber nichts an der Einstufung. Im Zweifel wird fachlicher Rat eingeholt.

14. Rollen und Verantwortlichkeiten

Rolle	Aufgaben
Geschäftsführung ([Name])	Trägt die Gesamtverantwortung, setzt die Richtlinie in Kraft, stellt Ressourcen und Schulungen bereit, entscheidet über Anwendungen mit hohem Risiko
KI-Verantwortliche/r ([Name, Funktion])	Pflegt Richtlinie und Tool-Register, nimmt Anträge entgegen, koordiniert Prüfungen, organisiert Schulungen, ist Ansprechperson bei Fragen
IT / Informationssicherheit ([Name])	Prüft Sicherheit, richtet Konten, Single Sign-on und Berechtigungen ein, überwacht Protokolle, begleitet Agenten und Schnittstellen
Datenschutzbeauftragte/r ([Name, intern oder extern])	Berät zu Rechtsgrundlagen, Auftragsverarbeitung und Folgenabschätzung, begleitet Betroffenenanfragen und Datenpannen
Betriebsrat (falls vorhanden)	Wird nach § 90 BetrVG unterrichtet und beteiligt, übt Mitbestimmungsrechte aus (Abschnitt 15)
Führungskräfte	Machen die Richtlinie bekannt, achten auf Einhaltung, fördern den sinnvollen Einsatz, sorgen für Schulung ihres Teams, behandeln Meldungen ohne Schuldzuweisung
Mitarbeitende	Halten die Richtlinie ein, prüfen Ergebnisse, melden Fehler und Vorfälle, besuchen Schulungen
Fachverantwortliche je Tool	Kennen Einstellungen und Bedingungen ihres Tools, melden Änderungen des Anbieters

Ein KI-Beauftragter im gesetzlichen Sinn ist nicht vorgeschrieben. Die Rolle der oder des KI-Verantwortlichen sorgt dafür, dass Entscheidungen einen festen Ansprechpunkt haben.

15. Betriebsrat

15.1 Das Unternehmen beteiligt den Betriebsrat nach dem Betriebsverfassungsgesetz an der Einführung und Anwendung von KI. Insbesondere gilt:

- Unterrichtung und Beratung über die Planung von Arbeitsverfahren und Arbeitsabläufen einschließlich des Einsatzes von KI (§ 90 BetrVG)
- Mitbestimmung bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, Verhalten oder Leistung der Beschäftigten zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG)
- Hinzuziehung eines Sachverständigen für KI, wenn der Betriebsrat die Einführung oder Anwendung beurteilen muss (§ 80 Abs. 3 BetrVG)
- Beteiligung bei Auswahlrichtlinien, auch wenn KI bei deren Erstellung eingesetzt wird (§ 95 Abs. 2a BetrVG)

15.2 Das Unternehmen setzt KI-Tools nicht zur Leistungs- oder Verhaltenskontrolle der Beschäftigten ein. Protokolle von KI-Tools, auch die von Agenten nach Abschnitt 11.4, werden nur zur Sicherheit, Fehlerbehebung und Kostenkontrolle ausgewertet, nicht personenbezogen zur Leistungsbewertung. Der Zugriff auf Protokolle ist auf [Rolle] beschränkt.

15.3 Wegen der Reichweite dieser Richtlinie bieten Geschäftsführung und Betriebsrat an, eine Betriebsvereinbarung zum Einsatz von KI abzuschließen. [Optional: Diese Richtlinie wird Bestandteil der Betriebsvereinbarung vom [Datum].] Sie regelt unter anderem: freigegebene Tools, verbotene Verwendungen, Auswertung von Nutzungsdaten, Schulungen, Verfahren bei Verstößen und Überprüfung.

15.4 [Wenn kein Betriebsrat besteht:] Die Beschäftigten können Fragen und Bedenken an [Name/Funktion] richten.

16. Verstöße und Meldungen

16.1 Fehler passieren. Wer einen Fehler macht oder einen Vorfall bemerkt, meldet ihn sofort an [E-Mail/Ticketsystem/Telefon]. Wer rasch meldet, hat keine Nachteile zu befürchten. Es geht um Schadensbegrenzung, nicht um Schuldzuweisung.

16.2 Zu melden sind insbesondere:

- Eingabe von Daten, die nicht in das Tool gehören (zum Beispiel Kundendaten in ein nicht freigegebenes Tool)
- Verlust oder Missbrauch von Zugangsdaten zu KI-Tools
- Ausgaben, die Dritten schaden könnten oder bereits fehlerhaft weitergegeben wurden
- Verdacht auf Prompt Injection oder auffälliges Verhalten eines Agenten
- Verstöße gegen diese Richtlinie durch andere, soweit sie Risiken bergen

16.3 Datenpannen. Haben Daten mit Personenbezug unbefugt ein KI-Tool oder einen Anbieter erreicht, informiert [Datenschutzbeauftragte/r] innerhalb von 24 Stunden die Geschäftsführung. Das Unternehmen prüft, ob eine Meldung an die Aufsichtsbehörde nötig ist. Eine Meldung muss nach Art. 33 DSGVO unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden erfolgen, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Betroffenen. Besteht ein hohes Risiko, sind auch die Betroffenen zu benachrichtigen (Art. 34 DSGVO). Die Frist beginnt, sobald das Unternehmen von der Verletzung Kenntnis hat. Deshalb ist die sofortige interne Meldung nach Abschnitt 16.1 wichtig.

16.4 Erste Maßnahmen: Eingabe stoppen, Verlauf und Dateien im Tool löschen, soweit möglich, Zugang sperren lassen, nichts verheimlichen.

16.5 Vorsätzliche oder grob fahrlässige Verstöße können arbeitsrechtliche Folgen haben. Versehen werden nicht sanktioniert, wenn sie umgehend gemeldet werden. Wiederholte

Verstöße trotz Hinweis, vorsätzliches Umgehen und das Verschweigen von Vorfällen werden dagegen nach den allgemeinen arbeitsrechtlichen Regeln behandelt.

16.6 Meldungen können auf Wunsch vertraulich erfolgen an [Name/Stelle].

17. Überprüfung und Inkrafttreten

17.1 [KI-Verantwortliche/r] prüft die Richtlinie mindestens einmal jährlich, erstmals am [Datum], und anlassbezogen bei neuen Tools, geänderten Anbieterbedingungen, Rechtsänderungen, Vorfällen oder neuen Erkenntnissen. Ergebnisse und Änderungen werden im Änderungsprotokoll festgehalten.

17.2 Das Tool-Register wird laufend gepflegt und mindestens [vierteljährlich] auf Aktualität geprüft. Die Aufbewahrung von Protokollen und Nachweisen (Schulung, Freigaben, Bestätigungen) richtet sich nach den gesetzlichen Fristen und dem Zweck. Personenbezogene Protokolle werden nicht länger als nötig gespeichert.

17.3 Diese Richtlinie tritt am [Datum] in Kraft. Frühere Regelungen zur KI-Nutzung treten außer Kraft. Sie wird allen Mitarbeitenden bekanntgemacht, die Kenntnisnahme wird bestätigt (Anhang E).

17.4 Sollten einzelne Regelungen unwirksam sein, bleiben die übrigen wirksam.

Ort, Datum	Unterschrift Geschäftsführung
[Ort, Datum]	[Name, Funktion]

Änderungsprotokoll:

Version	Datum	Änderung	Bearbeitet von
[1.0]	[Datum]	Ersterstellung	[Name]

Anhang A: Tool-Register (Vorlage)

Das Register wird laufend geführt. Alle Zeilen sind Beispiele in Platzhalterform und müssen durch Ihre eigenen Tools ersetzt werden. Nicht benötigte Zeilen löschen.

Tool	Version / Lizenz	Zulässige Zwecke	Höchste zulässige Datenklasse	Auflagen / Einstellungen	Verantwortlich	Freigegeben am
[Allgemeiner Chatassistent, z. B. Business- oder Enterprise-Tarif]	[Tarif, Anzahl Lizenzen, Vertrag vom Datum]	Texte entwerfen, Zusammenfassungen, Recherchehilfe, Ideen	[3 Vertraulich]	AVV abgeschlossen, Training aus, Verlauf [30] Tage, Anmeldung über SSO	[Name]	[Datum]
[Assistent in Office-Software, z. B. Copilot in Microsoft 365]	[Lizenz, Mandant]	E-Mail- und Dokumententwürfe, Besprechungszusammenfassungen	[4 Personenbezogen, nur im eigenen Mandanten]	Berechtigungen vorab prüfen, Aufzeichnung nur nach Ankündigung	[Name IT]	[Datum]
[Übersetzungstool mit Firmenvertrag]	[Tarif]	Übersetzung von Texten bis Klasse [2/3]	[3 Vertraulich]	Keine Speicherung der Texte, Verträge nur mit Prüfung	[Name]	[Datum]
[Entwicklungsassistent für Code]	[Lizenz]	Code-Vorschläge, Tests, Dokumentation	[3 Vertraulich, ohne Zugangsdaten]	Kern Quellcode nur nach Einzelfreigabe, Review durch zweite Person	[Name Entwicklung]	[Datum]
[Transkriptions- oder Meeting-Tool]	[Lizenz]	Protokolle von internen Besprechungen	[2 Intern]	Teilnehmende vorab informieren, keine Personalgespräche	[Name]	[Datum]
[Eigener Chatbot / Agent, z. B. für Auftragseingang]	[Plattform, Modell, Hosting]	[Beschreibung des Anwendungsfalls]	[Klasse, die in der Freigabe festgelegt ist]	Rechte, Protokoll, Bestätigung vor schreibenden Aktionen, Not-Aus	[Name]	[Datum]
[Bildgenerator mit Firmenvertrag]	[Tarif]	Illustrationen, Entwürfe für Marketing	[1 Öffentlich]	Kennzeichnung bei realistisch wirkenden Bildern, Rechteprüfung	[Name Marketing]	[Datum]

Anhang B: Antrag auf Freigabe eines KI-Tools oder Anwendungsfalls

Feld	Eintrag
Datum, antragstellende Person, Abteilung	
Name des Tools / Kurzbeschreibung des Anwendungsfalls	
Ziel: Was soll besser werden? (Zeit, Qualität, Kosten)	
Wer nutzt es, wie viele Personen?	
Anbieter, Tarif / Vertragsart (Unternehmensvertrag vorhanden?)	
Welche Daten sollen verarbeitet werden? (Datenklasse 1 bis 5, Beispiele)	
Enthalten die Daten personenbezogene Daten? Von wem (Kunden, Beschäftigte, Bewerber, Lieferanten)?	
Besondere Kategorien nach Art. 9 DSGVO oder Personalakten betroffen?	
Auftragsverarbeitungsvertrag vorhanden? Training aus? Speicherort bekannt?	
Anmeldung über Firmenkonto / SSO möglich?	
Greift das Tool auf andere Systeme zu (E-Mail, ERP, CRM, Dateiablage)? Lesend oder schreibend?	
Trifft oder beeinflusst das Tool Entscheidungen über Personen?	
Kommunikation mit Kunden oder Dritten in eigenem Namen (Chatbot, Telefon, E-Mail)?	
Wird jemand überwacht oder bewertet (Leistung, Verhalten, Stimmung)?	
Wie werden Ergebnisse geprüft? Wer prüft?	
Welche Risiken sehen Sie? Was passiert, wenn das Tool falsche Ergebnisse liefert?	
Kosten (einmalig, laufend)	
Gewünschter Start	

Ausfüllen durch Prüfende:

Prüfung	Ergebnis	Datum, Name
Risikostufe (niedrig / mittel / hoch)		
Datenschutz (AVV, Rechtsgrundlage, Folgenabschätzung nötig?)		
IT-Sicherheit (Anmeldung, Rechte, Protokoll)		
Betriebsrat informiert / beteiligt		
Hochrisiko-Einstufung nach KI-Verordnung geprüft		
Kennzeichnungspflicht nach Art. 50 geprüft		
Entscheidung: freigegeben / mit Auflagen / abgelehnt		

Prüfung	Ergebnis	Datum, Name
Auflagen / Begründung		
Eintrag im Tool-Register am		

Anhang C: Schulungsnachweis

Datum	Thema / Inhalt	Format (Präsenz, online, Selbststudium)	Dauer	Durchgeführt von	Teilnehmende (Name, Abteilung)	Unterschrift / Bestätigung
[Datum]	Grundschulung KI-Richtlinie, Datenklassen, Prüfpflicht	[Format]	[60 Minuten]	[Name / Anbieter]	[Name, Abteilung]	
[Datum]	Vertiefung [Personal / Vertrieb / Entwicklung / Agenten]	[Format]	[Dauer]	[Name / Anbieter]	[Name, Abteilung]	

Hinweis: Die Bundesnetzagentur empfiehlt, Art, Umfang und Teilnehmende der Maßnahmen zu dokumentieren. Aufbewahren Sie den Nachweis zusammen mit den Schulungsunterlagen.

Anhang D: Kurzfassung für alle Mitarbeitenden (eine Seite)

KI nutzen, aber sicher: die zehn Regeln bei [Firmenname]

1. Nur freigegebene Tools nutzen. Was im Tool-Register steht, ist erlaubt. Alles andere erst beantragen.
2. Nur mit dem Firmenkonto anmelden, nie mit privatem Konto oder privater E-Mail-Adresse.
3. Vorher die Datenklasse prüfen (1 öffentlich, 2 intern, 3 vertraulich, 4 personenbezogen, 5 streng vertraulich). Klasse 1 und 2 gehen in jedes freigegebene Tool. Klasse 3 und 4 nur, wenn das Register es für das Tool erlaubt. Klasse 5 nur mit schriftlicher Einzelfreigabe.
4. Keine personenbezogenen Daten ohne Freigabe. Namen entfernen reicht oft nicht, denken Sie an Kundennummern und Umstände.
5. Streng vertraulich bleibt draußen: Personalakten, Gesundheitsdaten, Gehälter, Konstruktionsdaten und Rezepturen des Kernprodukts, Zugangsdaten.
6. Jede Ausgabe prüfen. KI erfindet Zahlen, Quellen und Zitate. Wer sie verwendet, verantwortet sie.
7. Der Mensch entscheidet. Keine Entscheidung über Bewerbende, Beschäftigte oder Kunden allein durch KI.
8. Kennzeichnen, wo es nötig ist: Chatbots, echt wirkende KI-Bilder, -Videos und -Stimmen, KI-Texte zu Themen von öffentlichem Interesse ohne Prüfung.
9. Vorsicht bei fremden Dokumenten und Agenten. Dokumente aus unbekannter Quelle gehören nicht in Assistenten mit Zugriff auf Firmendaten. Agenten brauchen Freigabe.
10. Bei Fehlern, falsch eingegebenen Daten oder auffälligem Verhalten eines Tools sofort melden an [Stelle]. Wer schnell meldet, hat nichts zu befürchten. Bei Datenpannen zählt jede Stunde.

Fragen? [Name, E-Mail]. Neues Tool oder neue Idee? Antrag in Anhang B oder unter [Link]. Die vollständige Richtlinie finden Sie unter [Ort].

Anhang E: Bestätigung der Kenntnisnahme

Ich habe die KI-Richtlinie von [Firmenname] (Version [1.0], gültig ab [Datum]) und die Kurzfassung erhalten, gelesen und verstanden. Ich habe an der Einweisung teilgenommen oder werde sie vor der ersten Nutzung von KI-Tools absolvieren. Ich weiß, an wen ich mich bei Fragen und bei Vorfällen wende.

Name	Abteilung	Datum	Unterschrift

Bei elektronischer Bestätigung genügt eine dokumentierte Bestätigung im [System/Tool] mit Datum und Namen.

Diese Vorlage ist kostenlos. Sie dürfen sie nutzen, anpassen und weitergeben. Sie ersetzt keine Rechtsberatung.

Hilfe bei der Umsetzung: kostenlose KI-Potenzialanalyse unter kaluna-digital.de/ki-check/ · hallo@kaluna-digital.de