

VORLAGE · TOMORIS TOOLBOX

KI-Nutzungsrichtlinie: Vorlage für Unternehmen

Mustertext mit Platzhaltern, Rechtsrahmen nach KI-Verordnung in der Fassung des Digital Omnibus und DSGVO, Checkliste zur Einführung

STAND

25.10.2026

UMFANG

PDF, 10 Seiten

ONLINE

tomoris.com/downloads/ki-nutzungsrichtlinie-vorlage

AUF EINEN BLICK

Art. 4

KI-Kompetenz fördern:
Pflicht für jeden Betreiber

27.07.2026

Digital Omnibus zur KI in
Kraft, VO (EU) 2026/1744

02.08.2026

Transparenzpflichten
nach Art. 50 gelten

02.12.2027

Hochrisiko-Pflichten für
Anhang III, etwa Perso-
nalauswahl

FÜR WEN

- Geschäftsführung, die den Einsatz von KI-Assistenten regeln und verantworten will
- Datenschutzverantwortliche und Datenschutzbeauftragte
- IT-Leitung, die Werkzeuge wie Microsoft Copilot (bisher Microsoft 365 Copilot), ChatGPT oder Claude freigibt und absichert
- Personalabteilung, die Schulungen organisiert und KI im Personalbereich prüft

WURUM ES GEHT

Wer Beschäftigten KI-Assistenten bereitstellt, ist nach der KI-Verordnung Betreiber und muss die KI-Kompetenz des Personals fördern; seit 27. Juli 2026 gilt dafür die durch den Digital Omnibus geänderte Fassung von Art. 4. Dieses Dokument fasst den Rechtsrahmen mit Fundstellen zusammen und liefert einen Mustertext für eine interne KI-Nutzungsrichtlinie: Geltungsbereich, freigegebene Werkzeuge, Datenklassen, Prüfung der Ergebnisse, Kennzeichnung, Schulung, Meldewege und Verantwortliche. Eine Checkliste hilft bei der Einführung.

Diese Vorlage gibt einen Überblick und ersetzt keine Rechtsberatung. Maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung, insbesondere der KI-Verordnung samt Verordnung (EU) 2026/1744 und der DSGVO. Passen Sie den Mustertext an Ihr Unternehmen, Ihre Werkzeuge und Verträge an und stimmen Sie ihn intern ab, etwa mit Datenschutz und Betriebsrat.

INHALT

01	Wozu die Richtlinie dient	2
02	Der Rechtsrahmen in sechs Begriffen	3
03	Rechtsstand am 25. Oktober 2026	4
04	Mustertext, Teil 1: Geltung, Werkzeuge und Daten	5
05	Mustertext, Teil 2: Ergebnisse, Schulung und Verantwortung	6
06	Werkzeuge prüfen: was Hersteller zusagen	8
07	Checkliste: die Richtlinie einführen	8
08	Häufige Fehler	9
09	Quellen	10

01

Wozu die Richtlinie dient

Klare Regeln, welche KI-Werkzeuge erlaubt sind, welche Daten hineindürfen, wer Ergebnisse prüft und wer verantwortet.

Eine KI-Nutzungsrichtlinie legt fest, welche KI-Werkzeuge im Unternehmen erlaubt sind, wofür, mit welchen Daten und unter welcher Kontrolle. Das BSI empfiehlt, Beschäftigte darüber zu informieren, welche KI-Anwendungen sie zu welchen Zwecken verwenden, welche Eingaben sie tätigen und wie sie Ausgaben weiterverwenden dürfen. Diese Regeln sollen verbindlich, etwa in einer Richtlinie, festgehalten und technisch unterstützt werden, zum Beispiel durch das Sperren oder Freischalten bestimmter Dienste (BSI, Generative KI-Modelle, Version 2.0, Maßnahme M16).

Die KI-Servicestelle der RTR rät, die Ausrichtung des Unternehmens in einer internen KI-Richtlinie abzubilden: mit klaren Rollen, Verweisen auf andere Richtlinien, klar kommuniziert und für Mitarbeitende leicht auffindbar.

Um die Umsetzung von Art. 4 der KI-Verordnung belegen zu können, empfiehlt sie, KI-Strategie, Richtlinie und Schulungskonzept schriftlich festzuhalten und Schulungen je Person zu dokumentieren.

Eine schriftliche Richtlinie schreibt die KI-Verordnung nicht vor. Für Art. 4 verlangt die EU-Kommission weder ein Zertifikat noch einen KI-Beauftragten; Unternehmen können Schulungen und andere Maßnahmen intern dokumentieren (AI Literacy Q&A). Die Richtlinie ist das Werkzeug, mit dem Sie die Pflichten aus KI-Verordnung und DSGVO im Alltag umsetzen und nachweisen.

02

Der Rechtsrahmen in sechs Begriffen

Wer Betreiber ist, was Art. 4, 5, 26 und 50 der KI-Verordnung verlangen und welche DSGVO-Grundsätze gelten.

KI-Verordnung (EU) 2024/1689 in der Fassung der Verordnung (EU) 2026/1744, DSGVO

Betreiber

Betreiber ist, wer ein KI-System in eigener Verantwortung verwendet, außer im Rahmen einer persönlichen und nicht beruflichen Tätigkeit (Art. 3 Nr. 4). Stellt ein Unternehmen seinen Beschäftigten einen KI-Assistenten bereit, ist es Betreiber. Wer ein KI-System entwickelt oder entwickeln lässt und unter eigenem Namen in Verkehr bringt oder in Betrieb nimmt, etwa einen eigens entwickelten Chatbot, ist Anbieter (Art. 3 Nr. 3).

KI-Kompetenz (Art. 4)

Anbieter und Betreiber ergreifen Maßnahmen, um die Entwicklung der KI-Kompetenz ihres Personals und anderer Personen zu unterstützen, die in ihrem Auftrag KI-Systeme betreiben und nutzen. Zu berücksichtigen sind Kenntnisse, Erfahrung, Aus- und Fortbildung und der Einsatzkontext. Ein bestimmtes Kompetenzniveau müssen Sie für niemanden garantieren (Art. 4 Abs. 1). Die Pflicht gilt unabhängig von der Risikoklasse des Systems (RTR).

Verbotene Praktiken (Art. 5)

Verboten sind etwa manipulative Techniken, die erheblichen Schaden zufügen, Social Scoring und das Ableiten von Emotionen am Arbeitsplatz und in Bildungseinrichtungen, außer aus medizinischen oder Sicherheitsgründen (Art. 5 Abs. 1 lit. a, c und f). Ab 2. Dezember 2026 auch KI für intime Darstellungen bestimmbarer Personen ohne deren ausdrückliche Zustimmung und für Material nach RL 2011/93/EU; Betreibern ist nur die Verwendung zu diesem Zweck verboten (lit. ba, bb, Abs. 1a). Geldbußen bis 35 Mio. Euro oder 7 % des Weltumsatzes, der höhere Betrag, für KMU der niedrigere (Art. 99 Abs. 3, 6).

Transparenz (Art. 50)

Betreiber legen offen, dass Bild-, Ton- oder Videoinhalte künstlich erzeugt oder manipuliert sind, wenn es Deepfakes sind. Ebenso bei KI-Text, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, außer er wurde menschlich geprüft oder redaktionell kontrolliert und jemand trägt die redaktionelle Verantwortung (Art. 50 Abs. 4). Anbieter von Chatbots machen erkennbar, dass man mit einer KI interagiert (Abs. 1). Gilt seit 2. August 2026.

Hochrisiko-KI (Art. 26)

Betreiber von Hochrisiko-KI-Systemen verwenden sie nach Betriebsanleitung, übertragen die menschliche Aufsicht kompetenten Personen, überwachen den Betrieb, bewahren Protokolle mindestens sechs Monate auf und informieren vor dem Einsatz am Arbeitsplatz Arbeitnehmervertretung und Betroffene (Art. 26 Abs. 1, 2, 5, 6 und 7). Hochriskant sind etwa Systeme zur Bewerberauswahl oder Leistungsbewertung (Anhang III Nr. 4); für sie gelten diese Pflichten ab 2. Dezember 2027.

DSGVO-Grundsätze

Personenbezogene Daten verarbeiten Sie rechtmäßig und transparent, zweckgebunden, auf das Nötige beschränkt, richtig, nicht länger als nötig und sicher (Art. 5 Abs. 1 DSGVO); die Einhaltung müssen Sie nachweisen können (Abs. 2). Verarbeitet ein KI-Dienst Daten in Ihrem Auftrag, braucht es einen Auftragsverarbeiter mit hinreichenden Garantien (Art. 28 Abs. 1). Bei voraussichtlich hohem Risiko ist vorab eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 1).

03 —

Rechtsstand am 25. Oktober 2026

Der Digital Omnibus zur KI ist seit 27. Juli 2026 in Kraft. Was er für Betreiber ändert und welche Fristen jetzt gelten.

Die EU-Kommission hat den Digital Omnibus zur KI am 19. November 2025 vorgeschlagen. Beschlossen wurde er als Verordnung (EU) 2026/1744 vom 8. Juli 2026, veröffentlicht im Amtsblatt am 24. Juli 2026, in Kraft seit 27. Juli 2026 (Art. 4: dritter Tag nach der Veröffentlichung).

Geltungsbeginne nach Art. 113 KI-Verordnung in der Fassung der VO (EU) 2026/1744

●	●	●	●	●
2. Feb. 2025	2. Aug. 2026	2. Dez. 2026	2. Dez. 2027	2. Aug. 2028
KI-Kompetenz, Verbote	Transparenz, Aufsicht	Neue Verbote	Hochrisiko nach Anhang III	Hochrisiko nach Anhang I
Kapitel I und II gelten: Begriffe, KI-Kompetenz nach Art. 4 und verbotene Praktiken nach Art. 5 (Art. 113 Abs. 3 lit. a).	Allgemeiner Geltungsbeginn, unter anderem für Art. 50. Ab jetzt beaufsichtigen nationale Marktüberwachungsbehörden auch Art. 4 (EU-Kommission).	Verbote nach Art. 5 Abs. 1 lit. ba und bb. Anbieter bestehender Systeme kennzeichnen KI-Inhalte bis dahin maschinenlesbar (Art. 111 Abs. 4).	Kapitel III Abschnitte 1 bis 3, damit Art. 26, für Hochrisiko-Systeme nach Anhang III, etwa im Personalbereich (Art. 113 Abs. 3 lit. c).	Dieselben Pflichten für Hochrisiko-Systeme in Produkten nach Anhang I Abschnitt A, etwa Spielzeug oder Medizinprodukte (Art. 113 Abs. 3 lit. c); für Abschnitt B, etwa Maschinen, gilt Art. 2 Abs. 2.

Für Betreiber von KI-Assistenten zählt vor allem: Art. 4 verlangt nicht mehr, nach besten Kräften ein „ausreichendes Maß“ an KI-Kompetenz sicherzustellen, sondern Maßnahmen, die ihre Entwicklung unterstützen

(Art. 1 Nr. 5 VO 2026/1744). Art. 5 erhält zwei neue Verbote, die Hochrisiko-Pflichten beginnen später (Art. 1 Nr. 7 und 40). Art. 26 und Art. 50 Abs. 1 bis 4 blieben unverändert.

Nicht verwechseln: Parallel hat die Kommission auch Änderungen der DSGVO vorgeschlagen (Digital-Omnibus-Verordnung, COM(2025) 837). Dieses Verfahren 2025/0360/COD ist laut EUR-Lex am 25. Oktober 2026 noch nicht abgeschlossen. Es gilt die DSGVO in der bisherigen Fassung.

04

Mustertext, Teil 1: Geltung, Werkzeuge und Daten

Paragrafen 1 bis 4 mit Anlage 1 und 2. Ersetzen Sie alles in eckigen Klammern und streichen Sie, was nicht zutrifft.

So verwenden Sie den Mustertext: Ersetzen Sie die Platzhalter in eckigen Klammern, füllen Sie die Anlagen aus und stimmen Sie den Text mit Datenschutz, Informationssicherheit, Personalabteilung und, falls vorhanden, dem Betriebsrat ab. Die RTR nennt als bewährte Praxis eine interdisziplinäre Beobachtung durch Technik, Recht, Compliance, IT-Security, HR und Betriebsrat, je nach Unternehmensgröße.

KI-Nutzungsrichtlinie der [Unternehmen], Fassung [Version] vom [Datum]

§ 1 Zweck und Geltungsbereich

Diese Richtlinie regelt die Nutzung von KI-Werkzeugen bei [Unternehmen]. Sie gilt für alle Beschäftigten und für Personen, die in unserem Auftrag mit KI-Systemen arbeiten, etwa [Dienstleister, Leiharbeitskräfte], und für jede berufliche Nutzung, auch auf privaten Geräten. KI-Werkzeuge sind Anwendungen, die Texte, Bilder, Ton, Video oder Code erzeugen oder auswerten, einschließlich KI-Funktionen in bestehender Software.

§ 2 Freigegebene Werkzeuge

Beruflich verwenden Sie nur die Werkzeuge aus Anlage 1, mit dem dort genannten Konto und für die dort genannten Zwecke. Private Konten und Verbraucherversionen sind für Unternehmensdaten nicht zugelassen. Neue Werkzeuge und neue KI-Funktionen beantragen Sie bei [Stelle]; freigegeben wird nach Prüfung von Datenschutz, Vertrag und Sicherheit. Nicht freigegebene Dienste kann die IT sperren.

§ 3 Daten und Eingaben

Was Sie eingeben dürfen, richtet sich nach den Datenklassen in Anlage 2. Geben Sie nur ein, was für die Aufgabe nötig ist. Personenbezogene Daten, Geschäftsgeheimnisse und vertrauliche Kundendaten nur in Werkzeuge, die Anlage 1 dafür ausdrücklich freigibt. Gesundheitsdaten und andere besondere Kategorien nach Art. 9 DSGVO nur, wenn [Stelle] den konkreten Zweck freigegeben hat. Zugangsdaten und Passwörter nie.

§ 4 Zugriffe und selbstständige Aktionen

KI-Assistenten mit Zugriff auf E-Mails, Dateien oder andere Systeme können alles finden, was Sie selbst sehen dürfen. Melden Sie zu weit gefasste Freigaben an [IT-Stelle]. Funktionen, die selbstständig handeln, etwa E-Mails senden, Daten ändern oder Bestellungen auslösen, nutzen Sie nur, wenn [Stelle] sie freigegeben hat und jede Aktion vorher von Ihnen bestätigt wird.

Anlage 1: Freigegebene KI-Werkzeuge (zum Ausfüllen, Beispielzeile in eckigen Klammern)

WERKZEUG UND KONTO	ERLAUBTE ZWECKE	HÖCHSTE DATEN-KLASSE	VERANTWORTLICH
[z. B. Microsoft Copilot Chat mit Arbeitskonto]	[Entwürfe, Zusammenfassungen, Übersetzungen]	[intern]	[Name, Funktion]
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Anlage 2: Datenklassen und was in welches Werkzeug darf (an Ihre Klassifizierung anpassen)

DATENKLASSE	BEISPIELE	ERLAUBT IN
Öffentlich	veröffentlichte Texte, Website, Prospekte	allen Werkzeugen aus Anlage 1
Intern	Abläufe, Vorlagen, Entwürfe ohne Personen- oder Kundenbezug	Werkzeugen mit Unternehmenskonto: [Werkzeug]
Vertraulich	Angebote, Verträge, Kalkulationen, Quellcode, Geschäftsgeheimnisse	nur ausdrücklich freigegebenen Werkzeugen: [Werkzeug]
Personenbezogen	Namen, Kontaktdaten, Kundendaten, Personalunterlagen	nur Werkzeugen mit Auftragsverarbeitungsvertrag: [Werkzeug]
Besondere Kategorien, Zugangsdaten	Gesundheitsdaten und andere Daten nach Art. 9 DSGVO, Passwörter, Schlüssel	[keinem Werkzeug] oder nur nach Einzelfreigabe durch [Stelle]; Zugangsdaten nie

05

Mustertext, Teil 2: Ergebnisse, Schulung und Verantwortung

Paragrafen 5 bis 11 mit Anlage 3: menschliche Prüfung, Kennzeichnung, Rechte Dritter, Schulung, Meldung, Rollen, Überprüfung.

§ 5 Ergebnisse prüfen

KI-Ergebnisse können falsch, veraltet oder erfunden sein, auch wenn sie überzeugend klingen. Prüfen Sie jedes Ergebnis, bevor Sie es verwenden, und gleichen Sie Fakten, Zahlen, Zitate und Quellen ab. Inhalte mit Außenwirkung gibt [Rolle] vor der Veröffentlichung frei. Entscheidungen über Personen, etwa zu Bewerbungen, Leistung oder Kündigung, trifft ein Mensch; KI darf sie höchstens vorbereiten.

§ 6 Code und Konfigurationen

Von KI erzeugten Programmcode und Konfigurationen, etwa Firewallregeln oder Skripte, prüfen Sie vor dem Einsatz auf Fehler, Sicherheitslücken und veraltete Bibliotheken. Ausgaben, die direkt in andere Anwendungen, eine Kommandozeile oder einen Browser gehen, übernehmen Sie nie ungeprüft.

§ 7 Kennzeichnung

Wir kennzeichnen KI-erzeugte oder veränderte Bild-, Ton- und Videoinhalte, die echten Personen, Orten oder Ereignissen ähneln und echt wirken könnten (Deepfakes). KI-Texte, die wir zur Information der Öffentlichkeit über Angelegenheiten von öffentlichem Interesse veröffentlichen, kennzeichnen wir, es sei denn, sie wurden menschlich geprüft oder redaktionell kontrolliert und [Rolle] trägt dafür die redaktionelle Verantwortung (Art. 50 Abs. 4 KI-Verordnung). Chatbots für Kunden geben sich als KI zu erkennen. [Optional: weitere freiwillige Kennzeichnung]

§ 8 Rechte Dritter und Geschäftsgeheimnisse

Laden Sie fremde Texte, Bilder oder Code nur hoch, wenn wir sie für diesen Zweck nutzen dürfen. KI-Ergebnisse können geschützte Inhalte aus Trainingsdaten wiedergeben: Prüfen Sie Bilder und längere Textpassagen vor einer Veröffentlichung, bei Bildern etwa mit einer Rückwärtssuche. Vertrauliche Informationen von Kunden und Partnern behandeln Sie wie eigene; vertragliche Geheimhaltungspflichten gehen vor.

§ 9 Schulung

Wer KI-Werkzeuge nutzt, nimmt vor der ersten Nutzung an einer Einweisung teil und danach [jährlich] an einer Auffrischung. Inhalte sind mindestens: Funktionsweise und Grenzen, typische Fehler wie Halluzinationen und Verzerrungen, diese Richtlinie, die Werkzeuge aus Anlage 1 und die Meldewege. [Stelle] dokumentiert je Person Art, Inhalt und Ziel, Veranstalter, Datum und Wiederholungen.

§ 10 Fehler und Vorfälle melden

Melden Sie unverzüglich an [Kontakt]: Daten in einem nicht freigegebenen Werkzeug, fehlerhafte Ergebnisse mit Folgen, ungewöhnliches Verhalten eines Werkzeugs, etwa Anweisungen aus fremden Dokumenten, und unbeabsichtigte Aktionen. Sind personenbezogene Daten betroffen, prüft [Datenschutz] sofort, ob die Verletzung der Aufsichtsbehörde zu melden ist: unverzüglich und möglichst binnen 72 Stunden (Art. 33 Abs. 1 DSGVO).

§ 11 Verantwortung, Überprüfung, Geltung

Die Rollen nach Anlage 3 sind verbindlich. Führungskräfte sorgen dafür, dass ihre Teams die Richtlinie kennen. [Stelle] überprüft die Richtlinie und Anlage 1 mindestens [jährlich] sowie bei neuen Werkzeugen, neuen KI-Funktionen oder geänderter Rechtslage. Diese Richtlinie gilt ab [Datum], freigegeben durch [Name, Funktion]. [Optional: Folgen von Verstößen, abgestimmt mit HR und Betriebsrat]

Anlage 3: Rollen und Ansprechpersonen (zum Ausfüllen)

ROLLE	NAME, FUNKTION	VERTRETUNG
Verantwortlich für die Richtlinie	_____	_____
Freigabe neuer Werkzeuge und KI-Funktionen	_____	_____
Datenschutz	_____	_____
Informationssicherheit	_____	_____
Schulung und Dokumentation	_____	_____
Meldestelle für Fehler und Vorfälle	_____	_____

Warum § 8 wichtig ist: Ein Geschäftsgeheimnis ist nach § 26b Abs. 1 Z 3 UWG nur geschützt, wenn es Gegenstand angemessener Geheimhaltungsmaßnahmen ist. Regeln, welche vertraulichen Informationen in welche KI-Werkzeuge dürfen, können Teil solcher Maßnahmen sein.

06

Werkzeuge prüfen: was Hersteller zusagen

Zwei Beispiele aus der Hersteller-Dokumentation, Stand 25. Oktober 2026. Prüfen Sie jedes Werkzeug selbst, bevor es in Anlage 1 kommt.

Microsoft Copilot

So heißt Microsoft 365 Copilot inzwischen. Prompts, Antworten und über Microsoft Graph abgerufene Daten werden laut Microsoft nicht zum Training der Basismodelle verwendet. Copilot zeigt nur Unternehmensdaten, für die der Benutzer mindestens Anzeigeberechtigung hat; Microsoft rät, dafür die Berechtigungsmodelle etwa in SharePoint zu nutzen. Für EU-Kunden gilt die EU-Datengrenze, Modelle von Anthropic als Unterauftragsverarbeiter sind derzeit davon ausgenommen (Microsoft Learn).

Claude, kommerzielle Angebote

Eingaben und Ausgaben aus kommerziellen Produkten wie Claude for Work und der Anthropic API verwendet Anthropic standardmäßig nicht zum Training. Ausnahmen sind ausdrücklich gemeldetes Feedback, etwa über die Daumen-Schaltfläche, und eine sonstige Erlaubnis; Feedback wird samt Unterhaltung bis zu fünf Jahre gespeichert und kann in Team- und Enterprise-Plänen abgeschaltet werden. Für Verbraucherprodukte wie Claude Free, Pro und Max gelten eigene Regeln (Anthropic Privacy Center).

Herstellerangaben ändern sich. Maßgeblich sind Ihr Vertrag und die aktuelle Dokumentation; für andere Dienste, etwa ChatGPT, gelten deren eigene Bedingungen. Das BSI rät, Werkzeuge nach festgelegten Kriterien auszuwählen, etwa Funktionen, Trainingsdaten, Sicherheitsvorkehrungen, Haftung und Betrieb (Maßnahme M1). Halten Sie in Anlage 1 fest, welches Konto und welche Vertragsvariante freigegeben ist.

07

Checkliste: die Richtlinie einführen

Vierzehn Schritte von der Bestandsaufnahme bis zur regelmäßigen Überprüfung.

- ☐ Bestandsaufnahme: KI-Systeme und KI-Funktionen erfassen, auch in Standardsoftware und nach Updates (RTR).
- ☐ Rolle je Werkzeug klären: Betreiber oder, etwa beim eigenen Chatbot, Anbieter (Art. 3 Nr. 3 und 4).
- ☐ Zwecke prüfen: nichts nach Art. 5; Anhang-III-Zwecke wie Bewerberauswahl als Hochrisiko bewerten.

- ☐ Werkzeuge nach Kriterien auswählen: Funktionen, Datenverwendung, Sicherheit, Bedingungen (BSI M1).
- ☐ Verträge klären: Auftragsverarbeitung (Art. 28 DSGVO), Training mit Eingaben, Speicherort.
- ☐ Verarbeitungsverzeichnis ergänzen (Art. 30 DSGVO), Datenschutz-Folgenabschätzung prüfen (Art. 35).
- ☐ Berechtigungen bereinigen, bevor ein Assistent auf SharePoint, OneDrive oder Teams zugreift.
- ☐ Nicht freigegebene Dienste technisch sperren, freigegebene gezielt zulassen (BSI M16).
- ☐ Mustertext anpassen, mit Datenschutz, IT-Sicherheit, HR und Betriebsrat abstimmen, freigeben.
- ☐ Richtlinie bekanntmachen und für alle leicht auffindbar ablegen (RTR).
- ☐ Schulungen planen, durchführen und je Person dokumentieren, auch für Neueintritte (Art. 4, RTR).
- ☐ Meldeweg einrichten; festlegen, wer eine Meldung nach Art. 33 DSGVO prüft.
- ☐ Kennzeichnung nach Art. 50 Abs. 4 im Freigabeprozess für Veröffentlichungen verankern.
- ☐ Richtlinie und Anlage 1 regelmäßig und anlassbezogen überprüfen (RTR).

Mustertext und Checkliste sind Empfehlungen von TOMORIS. Gesetzlich vorgegeben sind die genannten Pflichten der KI-Verordnung und der DSGVO; eine bestimmte Form der Richtlinie schreibt keines der beiden Gesetze vor.

08

Häufige Fehler

Was eine Richtlinie wirkungslos macht und wie Sie es vermeiden.

- Richtlinie ohne Werkzeugliste: Ohne Anlage 1 ist unklar, was erlaubt ist.
- KI-Funktionen in bestehender Software übersehen: Auch Updates von Standardsoftware bringen oft neue KI-Komponenten mit (RTR).
- Berechtigungen nicht bereinigt: Microsoft Copilot nutzt Inhalte, auf die ein Benutzer zugreifen darf, also auch zu weit freigegebene Dateien (Microsoft Learn).
- Ergebnisse ungeprüft übernehmen: Überzeugende Ausgaben verleiten zu Automation Bias (BSI R8).
- Rechtsstand vor dem Digital Omnibus übernehmen: Art. 4 verlangt seit 27. Juli 2026 kein „ausreichendes Maß“ mehr; Hochrisiko-Pflichten nach Anhang III gelten erst ab 2. Dezember 2027.
- Datenschutz vergessen: Gelangen personenbezogene Daten unbefugt an Dritte, kann eine meldepflichtige Verletzung vorliegen (Art. 4 Nr. 12 und Art. 33 DSGVO).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- Verordnung (EU) 2024/1689 (KI-Verordnung), konsolidierte Fassung vom 27.07.2026, EUR-Lex**
Art. 3 Nr. 3 und 4; Art. 4, 5, 26, 50, 99, 111, 113; Anhang I und III; gelesen am 25.10.2026
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02024R1689-20...
- Verordnung (EU) 2026/1744 (Digital-Omnibus-Verordnung zur KI), ABL. L vom 24.7.2026**
Art. 1 Nr. 5, 7, 20, 39, 40 und Art. 4; gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu
- EUR-Lex: Verfahren 2025/0360/COD, Digital-Omnibus-Verordnung (COM(2025) 837)**
Status „Ongoing“, abgerufen am 25.10.2026
eur-lex.europa.eu/procedure/DE/2025_360
- Verordnung (EU) 2016/679 (DSGVO), EUR-Lex**
Art. 4 Nr. 12, Art. 5, 9, 28, 30, 33, 35
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- EU-Kommission: AI Literacy – Questions & Answers**
Stand 20.10.2026, gelesen am 25.10.2026
digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-ans...
- RTR KI-Servicestelle: KI-Kompetenz**
Abschnitte Umsetzung, Operative Umsetzung, Dokumentation; gelesen am 25.10.2026
www.rtr.at/rtr/service/ki-servicestelle/ai-act/ki-kompetenz.de...
- BSI: Generative KI-Modelle – Chancen und Risiken für Industrie und Behörden, Version 2.0**
Version 2.0 vom 17.01.2025; Risiken R3 bis R6 und R8, Maßnahmen M1, M16 bis M18, M20
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Mo...
- Microsoft Learn: Daten, Datenschutz und Sicherheit für Microsoft Copilot**
Abschnitte Organisationsdaten, EU-Datengrenze, Schutz; gelesen am 25.10.2026
learn.microsoft.com/de-de/microsoft-365/copilot/microsoft-365-c...
- Anthropic Privacy Center: Is my data used for model training? (kommerzielle Produkte)**
Stand 18.8.2026, gelesen am 25.10.2026
privacy.claude.com/en/articles/7996868-is-my-data-used-for-mode...
- Bundesgesetz gegen den unlauteren Wettbewerb (UWG), § 26b, RIS**
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...