SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

Europe Cyber-Safe

KI-Betreiber-Pass — Erklärung zur Selbstbewertung

Organisation	Beispiel Kreativagentur GmbH (15 Mitarbeitende)	**Referenz**	SAMPLE-0002
Ausgefüllt am	2026-10-30	**Ausgefüllt von**	director@example.com
Fragenkatalog	v1.1-EU-de (EU, de) · `4f08ba4ceaccb6c8`		

> **Von der Organisation ausgefüllte Selbstbewertung. Die Antworten wurden weder von Europe Cyber-Safe noch von Dritten untersucht. Dieser Bericht ist keine Rechtsberatung.**

Der Bericht beschreibt ausschließlich den Stand zum Datum des Ausfüllens.

Bewertungen der Bereiche

Jeder Bereich wird anhand der gegebenen Antworten bewertet: rot, wenn eine Antwort ein Rot-Auslöser ist, sonst gelb, wenn eine Antwort gelb oder unbeantwortet ist, sonst grün. Es wird keine Gesamtpunktzahl ermittelt.

Bereich	Bewertung
D1 KI-Inventar	ROT
D2 Datenschutz	ROT
D3 Governance und Richtlinien	ROT
D4 Menschliche Aufsicht	GELB
D5 Anbietermanagement	GELB
D6 Reaktion auf KI-Vorfälle	GELB

Maßnahmen

Rote Bereiche zuerst, danach die schnellsten Maßnahmen zuerst.

#	Bereich	Maßnahme	Aufwand
1	D1	Benennen Sie eine verantwortliche Person für das Inventar und halten Sie dies in der KI-Nutzungsrichtlinie fest.	eine Stunde
2	D1	Tragen Sie einen vierteljährlichen Inventarabgleich in den Kalender der benannten verantwortlichen Person ein.	eine Stunde
3	D2	Ergänzen Sie die Datenschutzerklärung um einen Abschnitt zur KI-Nutzung mit Zwecken und Kategorien von Anbietern; veröffentlichen Sie ihn und informieren Sie die Mitarbeitenden.	eine Stunde
4	D2	Verteilen Sie die Liste „Nicht eingeben“ an alle Mitarbeitenden und hängen Sie sie dort aus, wo die Tools genutzt werden.	eine Stunde

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

5	D2	Halten Sie für jedes Tool anhand der Anbieterdokumentation Datenstandort und Übermittlungsmechanismus fest; wenn Daten den EWR verlassen, klären Sie den Mechanismus (ein Angemessenheitsbeschluss oder EU-Standardvertragsklauseln mit einer Bewertung der Übermittlung).	eine Stunde
6	D2	Ermitteln Sie für jedes Tool die Löschfunktion oder die vertragliche Löschzusage; entfernen Sie Tools, bei denen es keines von beiden gibt und personenbezogene Daten betroffen sind.	eine Stunde
7	D3	Benennen Sie eine für KI-Entscheidungen verantwortliche Person und halten Sie die drei Fragen fest, die sie vor der Zulassung eines Tools stellt (welche Daten, welche Bedingungen, wer kontrolliert die Ergebnisse).	eine Stunde
8	D1	Vervollständigen Sie das KI-Inventar anhand der Vorlage; fragen Sie jede Teamleitung, welche Tools sie und ihr Team nutzen, einschließlich Browsererweiterungen und Smartphone-Apps.	ein Tag
9	D1	Geben Sie ab sofort keine personenbezogenen Daten mehr in Tools mit Verbraucher- oder unbekannten Bedingungen ein. Verlagern Sie diese Nutzung entweder in eine Business-Variante mit Auftragsverarbeitungsvertrag, oder stellen Sie die Nutzung ein.	ein Tag
10	D1	Prüfen Sie die KI-Einstellungen jedes wichtigen Produkts (Meeting-Transkription, Zusammenfassung, Autovervollständigung) und nehmen Sie sie in das Inventar auf; entscheiden Sie, welche Funktionen deaktiviert werden.	ein Tag
11	D2	Führen Sie für jedes Tool, das personenbezogene Daten berührt, die DSFA-Vorprüfung anhand der Vorlage durch; erstellen Sie eine vollständige DSFA, wo die Vorprüfung dies ergibt.	ein Tag
12	D3	Übernehmen Sie die Vorlage für die KI-Nutzungsrichtlinie (zwei Seiten), lassen Sie sie von der verantwortlichen Person unterzeichnen, geben Sie sie an alle Mitarbeitenden heraus und halten Sie fest, wer sie zur Kenntnis genommen hat.	ein Tag
13	D3	Führen Sie für alle Mitarbeitenden eine einstündige KI-Sensibilisierung durch (Präsentationsvorlage) und bewahren Sie die Teilnahmeliste auf.	ein Tag
14	D3	Prüfen Sie die fünf wichtigsten Mandanten- bzw. Kundenverträge und die KI-Leitlinien Ihrer Berufskammer oder Ihres Berufsverbands auf Vertraulichkeits- und KI-Klauseln; dokumentieren Sie das Ergebnis.	ein Tag
15	D4	Informieren Sie die Mitarbeitenden anhand des einseitigen Merkblatts über typische KI-Fehler; nehmen Sie ein reales Beispiel aus Ihrer eigenen Branche auf.	eine Stunde
16	D4	Vereinbaren Sie eine einfache Konvention (eine Fußzeile, ein Feld, ein Ordner), um relevante KI-gestützte Ergebnisse zu kennzeichnen.	eine Stunde
17	D5	Prüfen Sie die Angaben jedes Anbieters zur Datennutzung; aktivieren Sie das Opt-out oder wechseln Sie zu einer Variante ohne Training; halten Sie das Ergebnis im Inventar fest.	eine Stunde
18	D5	Sammeln Sie für jeden Anbieter die Nachweise von dessen Sicherheitsseite oder Trust Center und bewahren Sie sie zusammen mit dem Inventar auf.	eine Stunde

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

19	D5	Legen Sie fest, wer Anbietermitteilungen erhält; verfassen Sie für jedes kritische Tool eine Ausstiegsnotiz von einem Absatz (wie exportieren, wie beenden).	eine Stunde
20	D6	Nehmen Sie KI-Vorfälle mit drei Beispielen und einer benannten Ansprechperson in das bestehende Vorfall- oder Beschwerdeverfahren auf.	eine Stunde
21	D6	Benennen Sie die Person, die über Datenpannen entscheidet, und halten Sie das Meldeformular Ihrer Datenschutzaufsichtsbehörde sowie eine Vorlage für ein Verzeichnis der Datenpannen bereit (Art. 33 DSGVO verlangt eine Dokumentation jeder Datenpanne).	eine Stunde
22	D6	Aktivieren Sie die Aktivitätsprotokollierung in Business-Tools; wo dies nicht möglich ist, führen Sie ein einfaches gemeinsames Protokoll für Nutzungen mit personenbezogenen oder vertraulichen Daten.	eine Stunde
23	D4	Führen Sie für alle kundenwirksamen und für Unterlagen relevanten KI-Ergebnisse einen Kontrollschritt durch eine benannte Person ein; machen Sie ihn zum Teil der üblichen Abzeichnung.	ein Tag
24	D5	Beschaffen Sie für jeden Anbieter die Business-Bedingungen oder den AVV; wo keine vorliegen, senden Sie diesem Anbieter keine personenbezogenen Daten mehr.	ein Tag
25	D5	Stellen Sie KI-Tools auf vom Unternehmen verwaltete Konten mit MFA um; nehmen Sie sie in die Offboarding-Checkliste auf.	ein Tag
26	D6	Testen Sie für jedes kritische Tool einmal den Export und halten Sie fest, wie der Zugang deaktiviert wird; bewahren Sie wesentliche Unterlagen außerhalb des Tools auf.	ein Tag
27	D4	Dokumentieren Sie den Kontrollschritt, die Rechtsgrundlage und die durchgeführten Bias-Prüfungen; entscheiden Sie, ob die Nutzung unter Anhang III der KI-Verordnung fällt, und planen Sie die Betreiberpflichten ein, die ab dem 2. Dezember 2027 gelten.	eine Woche

Gegebene Antworten

D1 KI-Inventar — ROT

ID	Frage	Antwort	Stufe
D1-1	Haben Sie alle im Unternehmen genutzten KI-Tools erfasst, einschließlich kostenloser Konten, die Mitarbeitende auf eigenen Geräten oder mit eigenen Zugangsdaten nutzen?	Keine Liste	rot
D1-2	Erhält ein Tool im Inventar personenbezogene Daten von Kunden, Patienten, Mandanten oder Beschäftigten?	Ja - in mindestens einem Tool mit Verbraucherbedingungen oder mit unbekannten Bedingungen	rot
D1-3	Gibt es eine namentlich benannte Person, die das Inventar aktuell hält und über die Zulassung neuer Tools entscheidet?	Nein	gelb

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

D1-4	Sind KI-Funktionen, die in bereits genutzte Produkte integriert sind (E-Mail, CRM, Buchhaltung, Browser, Meeting-Tools, Telefone), im Inventar enthalten?	Nicht sicher	gelb
D1-5	Wann wurde das Inventar zuletzt mit der tatsächlichen Nutzung durch die Mitarbeitenden abgeglichen?	Nie, oder kein Inventar	rot

D2 Datenschutz — ROT

ID	Frage	Antwort	Stufe
D2-1	Informiert Ihre Datenschutzerklärung Kunden und Beschäftigte darüber, dass KI-Tools eingesetzt werden, wofür und mit welchen Anbietern?	Nein	rot
D2-2	Haben Sie für Tools, die personenbezogene Daten verarbeiten, eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt oder eine dokumentierte Vorprüfung, die ergeben hat, dass keine erforderlich ist?	Nein	rot
D2-3	Haben die Mitarbeitenden eine schriftliche Liste dessen, was niemals in ein KI-Tool eingegeben werden darf (zum Beispiel Patientendaten, Kartennummern, Mandantenkennungen, Passwörter)?	Mündlich mitgeteilt, nichts Schriftliches	gelb
D2-4	Wissen Sie, wo jeder Anbieter Ihre Daten speichert und verarbeitet und ob sie den Europäischen Wirtschaftsraum (EWR) verlassen?	Für einige Tools	gelb
D2-5	Können Sie in einem KI-Tool gespeicherte Daten löschen oder vom Anbieter löschen lassen, wenn Sie die Nutzung beenden oder eine Person dies verlangt?	Nicht sicher	gelb

D3 Governance und Richtlinien — ROT

ID	Frage	Antwort	Stufe
D3-1	Gibt es eine schriftliche KI-Nutzungsrichtlinie, die den Mitarbeitenden bekannt ist und festlegt, was erlaubt ist und was nicht?	Entworfen, aber nicht herausgegeben	gelb
D3-2	Wer entscheidet, ob ein neues KI-Tool oder eine neue KI-Funktion für geschäftliche Zwecke genutzt werden darf?	Die Geschäftsleitung, informell	gelb

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

D3-3	Führt die Richtlinie verbotene Nutzungen auf - zum Beispiel Entscheidungen über Personen ohne menschliche Kontrolle oder das Erzeugen von Inhalten, die als von Menschen verfasst ausgegeben werden, wo dies irreführen würde?	Ja	grün
D3-4	Haben alle Mitarbeitenden, die KI-Tools nutzen, in den letzten 12 Monaten eine Sensibilisierungsschulung zu Eingabegrenzen, typischen Fehlerarten und der Richtlinie erhalten?	Einige Mitarbeitende	gelb
D3-5	Schränken Verträge mit Mandanten oder Kunden, Berufsregeln oder Ihre Aufsichtsbehörde ein, wie Sie KI mit deren Informationen nutzen dürfen, und halten Sie diese Vorgaben ein?	Es gibt Einschränkungen, und wir sind nicht sicher, ob wir sie einhalten	rot

D4 Menschliche Aufsicht — GELB

ID	Frage	Antwort	Stufe
D4-1	Werden KI-Ergebnisse von einer fachkundigen Person kontrolliert, bevor sie an Kunden gehen, in Unterlagen einfließen oder in eine Entscheidung über eine Person eingehen?	Meistens	gelb
D4-2	Kennen die Mitarbeitenden, die KI-Tools nutzen, die typischen Fehler dieser Tools - erfundene Fakten und Quellenangaben, veraltete Informationen, selbstsicher vorgetragene Fehler, Verzerrungen (Bias)?	Einige Mitarbeitende	gelb
D4-3	Können Sie im Nachhinein erkennen, welche Dokumente, E-Mails oder Datensätze mit KI-Unterstützung entstanden sind?	Manchmal	gelb
D4-4	Ist für eine KI-gestützte Entscheidung eine namentlich benannte Person genauso verantwortlich wie für eine menschliche Entscheidung?	Ja	grün
D4-5	Nutzen Sie KI für Personalauswahl, Kreditvergabe, Preisgestaltung, Anspruchsentscheidungen, Leistungsbeurteilung oder andere Entscheidungen über Einzelpersonen?	Ja, mit echter menschlicher Kontrolle und dokumentierter Grundlage	gelb

D5 Anbietermanagement — GELB

ID	Frage	Antwort	Stufe

D5-1	Haben Sie für jeden KI-Anbieter, der Ihre Daten verarbeitet, einen Vertrag oder Bedingungen, die einen Auftragsverarbeitungsvertrag (AVV) umfassen?	Für einige	gelb
D5-2	Wissen Sie, ob jeder Anbieter Ihre Eingaben zum Training oder zur Verbesserung seiner Modelle nutzt, und haben Sie, wo möglich, widersprochen (Opt-out)?	Unbekannt	gelb
D5-3	Haben Sie von jedem Anbieter unabhängige Sicherheitsnachweise gesehen (zum Beispiel ein ISO/IEC 27001-Zertifikat, einen SOC 2-Bericht, ein nationales Grundschutz-Programm, eine Zusammenfassung eines Penetrationstests)?	Nein	gelb
D5-4	Wird der Zugang zu jedem KI-Tool über Firmenkonten, Multi-Faktor-Authentifizierung und Entzug beim Ausscheiden von Mitarbeitenden gesteuert?	Teilweise	gelb
D5-5	Würden Sie es erfahren, wenn ein Anbieter seine Bedingungen ändert, eine Datenpanne hat oder den Betrieb einstellt, und können Sie die Nutzung schnell beenden?	Nein	gelb

D6 Reaktion auf KI-Vorfälle — GELB

ID	Frage	Antwort	Stufe
D6-1	Wissen die Mitarbeitenden, was als KI-Vorfall gilt (zum Beispiel in ein Tool eingefügte personenbezogene Daten, eine schädliche oder falsche Ausgabe, auf deren Grundlage gehandelt wurde, eine Mitteilung des Anbieters über eine Datenpanne), und wie sie ihn melden?	Informell	gelb
D6-2	Könnten Sie die 72-Stunden-Meldefrist der DSGVO gegenüber Ihrer Datenschutzaufsichtsbehörde einhalten, wenn personenbezogene Daten über ein KI-Tool offengelegt würden?	Nicht sicher	gelb
D6-3	Hatten Sie in den letzten 12 Monaten einen KI-Vorfall, oder haben Sie dafür eine Planspielübung (Tabletop) durchgeführt?	Ja	grün
D6-4	Führen Sie ausreichende Aufzeichnungen (wer hat welches Tool wann wofür genutzt), um einen KI-Vorfall im Nachhinein untersuchen zu können?	Teilweise	gelb

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG

D6-5	Könnten Sie die Nutzung eines bestimmten KI-Tools innerhalb eines Arbeitstags beenden, wenn es kompromittiert wäre, ohne wesentliche Geschäftsunterlagen zu verlieren?	Teilweise	**gelb**

Herangezogene Leitlinien

- KI-Verordnung, Art. 26 (Pflichten der Betreiber von Hochrisiko-KI-Systemen) und Anhang III; für Nutzungen nach Anhang III gelten diese ab dem 2. Dez. 2027 gemäß Verordnung (EU) 2026/1744
- KI-Verordnung (Verordnung (EU) 2024/1689), Art. 4 (KI-Kompetenz), anwendbar seit dem 2. Feb. 2025 und geändert durch Verordnung (EU) 2026/1744: Anbieter und Betreiber müssen Maßnahmen ergreifen, um die KI-Kompetenz ihres Personals und anderer Personen zu fördern, die in ihrem Auftrag KI-Systeme nutzen
- KI-Verordnung, Art. 50 (Transparenz: Personen darüber informieren, dass sie mit einem KI-System interagieren; KI-generierte oder manipulierte Inhalte offenlegen), anwendbar seit dem 2. Aug. 2026
- ISO/IEC 27001:2022; nationale Grundschutz-Programme (zum Beispiel BSI IT-Grundschutz, CyberFundamentals); Multi-Faktor-Authentifizierung und Kontrollen bei Eintritt und Austritt von Mitarbeitenden
- Europäische Kommission, KI-Kompetenz - Fragen und Antworten (2025)
- Europäischer Datenschutzausschuss (EDSA), Stellungnahme 28/2024 zu bestimmten Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen (Dez. 2024); KI-Leitlinien, veröffentlicht durch die zuständige Datenschutzaufsichtsbehörde (z. B. die BfDI oder Ihre Landesdatenschutzbehörde)
- Nationales Arbeitsrecht und Mitbestimmungsregeln (Betriebsrat) zur Überwachung und zum KI-Einsatz bei Personalauswahl und Personalführung; KI-Verordnung, Anhang III Nummer 4 (Nutzungen im Beschäftigungsbereich gelten als hochriskant)
- ENISA, Multilayer Framework for Good Cybersecurity Practices for AI (2023); NCSC/CISA und Partnerbehörden, Guidelines for secure AI system development (Nov. 2023)
- EU-Gleichbehandlungsrichtlinien (2000/43/EG, 2000/78/EG, 2006/54/EG) und nationales Antidiskriminierungsrecht (unmittelbare und mittelbare Diskriminierung)
- DSGVO, Art. 22 (automatisierte Entscheidungen im Einzelfall); Leitlinien der Artikel-29-Datenschutzgruppe zu automatisierten Entscheidungen im Einzelfall und Profiling (WP251 rev.01)
- DSGVO, Art. 33-34 (Meldung an die Aufsichtsbehörde binnen 72 Stunden, wenn ein Risiko für Personen besteht; Dokumentation jeder Datenpanne); EDSA-Leitlinien 9/2022 zur Meldung von Verletzungen des Schutzes personenbezogener Daten
- DSGVO, Art. 35 (Datenschutz-Folgenabschätzung); DSFA-Leitlinien der Artikel-29-Datenschutzgruppe (WP248 rev.01, vom EDSA übernommen); Liste Ihrer nationalen Aufsichtsbehörde mit Verarbeitungsvorgängen, für die eine DSFA durchzuführen ist
- DSGVO, Kapitel V (Art. 44-49): Angemessenheitsbeschlüsse; Standardvertragsklauseln (Beschluss 2021/914 der Kommission); Empfehlungen 01/2020 des EDSA zu ergänzenden Maßnahmen
- Datenschutz-Grundverordnung (DSGVO), Art. 12-14 (den betroffenen Personen bereitzustellende Informationen)
- ENISA-Leitfäden zur Bearbeitung von Sicherheitsvorfällen; Meldehinweise Ihres nationalen CSIRT; Meldepflichten nach NIS-2-Richtlinie, Art. 23 (für erfasste Einrichtungen)
- ISO/IEC 42001:2023, KI-Managementsysteme (Rollen, Folgenabschätzung, Lebenszyklus, Lieferanten)
- ISO/IEC 27001:2022 Anhang A 8.15 (Protokollierung) und 8.16 (Überwachungstätigkeiten)
- NIST AI Risk Management Framework 1.0 (Govern, Map, Measure, Manage) und das zugehörige Generative AI Profile (NIST AI 600-1)
- OWASP Top 10 for LLM Applications 2025 (Prompt Injection, Offenlegung sensibler Informationen, Lieferkette)
- ENISA-Leitfäden zur Sicherheit der IKT-Lieferkette; NIS-2-Richtlinie, Art. 21(2)(d) Sicherheit der Lieferkette (für erfasste Einrichtungen)

Die Leitlinienverweise sind öffentliche Quellen, die der Einfachheit halber aufgeführt sind; prüfen Sie die aktuelle Fassung, bevor Sie sich darauf stützen. Diese Erklärung ist keine Rechtsberatung und kein Zertifikat.

SYNTHETISCHES BEISPIEL — KEINE KUNDENBEWERTUNG