

Checkliste: DSGVO-konforme KI-Einführung im Unternehmen

Checkliste von Vryne — ausführlich erklärt unter <https://vryne.com/ratgeber/dsgvo-konforme-ki-einfuehren>
Stand: 28. Oktober 2026. Allgemeiner Überblick, keine Rechtsberatung — die Prüfung des Einzelfalls durch eure Datenschutzbeauftragten ersetzt sie nicht.

Unternehmen: [Unternehmen] · Werkzeug: [Name des KI-Werkzeugs] · Verantwortlich: [Name] ·
Datum: [Datum]

1. Zweck und Rechtsgrundlage

- ☐ Anwendungsfälle konkret beschrieben (nicht „KI für alle“)
- ☐ Datenkategorien festgehalten: interne Dokumente ohne Personenbezug, Kundendaten, Beschäftigendaten, besondere Kategorien (Art. 9 DSGVO)
- ☐ Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO je Verarbeitung bestimmt
- ☐ Für Beschäftigendaten Art. 88 DSGVO / § 26 BDSG mit dem Datenschutzbeauftragten abgestimmt
- ☐ Datenminimierung geprüft: Was nicht gebraucht wird, kommt nicht ins System
- ☐ Speicherdauer für Dokumente, Chatverläufe und Protokolle festgelegt

2. Anbieters Auswahl

- ☐ Sitz des Anbieters in der EU (Gerichtsstand, anwendbares Recht)
- ☐ Serverstandort je Schicht geprüft: Anwendung, Datenbank, Dokumentenablage, Backups, Sprachmodelle
- ☐ Drittlandtransfer (Art. 44 ff. DSGVO) ausgeschlossen oder abgesichert (Angemessenheitsbeschluss bzw. Standardvertragsklauseln mit Transfer-Folgenabschätzung)
- ☐ Konzernzugehörigkeit geprüft: Unterliegt der Anbieter dem US CLOUD Act?
- ☐ Training mit Kundendaten vertraglich ausgeschlossen — auch für Eingaben und Antworten
- ☐ Liste der Unterauftragsverarbeiter mit Sitz, Zweck und Verarbeitungsort liegt vor
- ☐ Löschung und Export bei Vertragsende geklärt (Dokumente, Vektoren, Backups)

3. Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

- ☐ AVV abgeschlossen
- ☐ Mindestinhalte nach Art. 28 Abs. 3 DSGVO enthalten (Gegenstand, Dauer, Art und Zweck, Datenarten, Weisungen, Vertraulichkeit)
- ☐ TOM-Anlage liegt vor und wurde geprüft

- ☐ Modellanbieter sind als Unterauftragsverarbeiter genannt
- ☐ Unterstützung bei Betroffenenrechten und Datenpannen geregelt
- ☐ Nachweis- und Kontrollrechte geregelt

4. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

- ☐ Eintrag für die KI-Nutzung angelegt
- ☐ Zweck, betroffene Personen und Datenkategorien eingetragen
- ☐ Empfänger inkl. Anbieter und Unterauftragsverarbeiter eingetragen
- ☐ Drittlandtransfers (oder deren Ausschluss) eingetragen
- ☐ Löschfristen und Verweis auf die TOMs eingetragen

5. Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

- ☐ Schwellwertanalyse durchgeführt und dokumentiert
- ☐ Muss-Liste der Aufsichtsbehörden (DSK) geprüft
- ☐ Risikofaktoren geprüft: besondere Kategorien, Bewertung von Personen, Überwachung von Beschäftigten, Entscheidungen mit erheblicher Wirkung
- ☐ Falls erforderlich: DSFA durchgeführt
- ☐ Datenschutzbeauftragter einbezogen (Art. 35 Abs. 2 DSGVO)

6. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- ☐ Rollen- und Rechtekonzept: Wer sieht welche Dokumente?
- ☐ Getrennte Bereiche für vertrauliche Unterlagen
- ☐ Verschlüsselung bei Übertragung und Speicherung bestätigt
- ☐ Protokollierung und Regel zum Zugriff auf Protokolle festgelegt
- ☐ Löschkonzept für Dokumente, Chatverläufe und Backups
- ☐ Ablauf für Datenpannen (Meldung binnen 72 Stunden, Art. 33 DSGVO)

7. Betriebsrat (§ 87 Abs. 1 Nr. 6 BetrVG)

- ☐ Betriebsrat frühzeitig unterrichtet (§ 90 BetrVG)
- ☐ Hinzuziehung eines Sachverständigen angeboten bzw. geklärt (§ 80 Abs. 3 BetrVG)
- ☐ Betriebsvereinbarung abgeschlossen: Zweck, Werkzeuge, Ausschluss von Leistungs- und Verhaltenskontrolle, Zugriff auf Protokolle, Schulung

8. Schulung und KI-Kompetenz (Art. 4 KI-Verordnung)

- ☐ Bestandsaufnahme der genutzten KI-Systeme (auch privat beschaffte)
- ☐ Schulungskonzept: Basismodul für alle, Vertiefung je Rolle
- ☐ Inhalte: Funktionsweise und Grenzen, verbotene Eingaben, Prüfpflicht, Kennzeichnung
- ☐ Teilnahme dokumentiert (wer, wann, welche Inhalte)

9. KI-Richtlinie

- ☐ Richtlinie erstellt (Vorlage: <https://vryne.com/downloads/ki-richtlinie-vorlage.md>)
- ☐ Liste der freigegebenen Werkzeuge als Anlage gepflegt
- ☐ Mit Datenschutz, IT und Betriebsrat abgestimmt
- ☐ Bekannt gemacht, Kenntnisnahme dokumentiert

10. Pilot und Rollout

- ☐ Pilotgruppe und Dokumentenbestand festgelegt
 - ☐ Auswertungskriterien festgelegt: Richtigkeit, nachvollziehbare Quellen, Fehleingaben, Datenschutzfragen
 - ☐ Pilot ausgewertet und dokumentiert
 - ☐ Rollout in Stufen geplant
 - ☐ Verzeichnis, TOMs und Richtlinie nach dem Pilot aktualisiert
 - ☐ Regelmäßige Überprüfung terminiert (mindestens jährlich und bei neuen Werkzeugen)
-

Weitere Ratgeber: <https://vryne.com/ratgeber>