bridge to ai

KI-STARTER-CHECKLISTE · FÜR KLEINE & MITTLERE UNTERNEHMEN

KI *sicher* & DSGVO-konform einsetzen

Die kompakte Schritt-für-Schritt-Checkliste, mit der Sie KI im Unternehmen einführen, ohne rechtliche Risiken einzugehen – verständlich, ohne Tech-Jargon.

KI spart enorm viel Zeit – aber nur, wenn Datenschutz und Sicherheit von Anfang an mitgedacht werden. Diese Checkliste führt Sie durch die **wichtigsten Prüfpunkte**, bevor und während Sie KI-Tools nutzen. Haken Sie ab, was bereits erfüllt ist – so sehen Sie sofort, wo noch Handlungsbedarf besteht.

01 Grundlagen klären – bevor das erste Tool startet

- [ ] Verantwortlichkeit benennen: Wer im Unternehmen entscheidet über KI-Einsatz und Datenschutz?
- [ ] Übersicht erstellen: Welche KI-Tools werden bereits genutzt – auch inoffiziell durch Mitarbeitende („Schatten-KI“)?
- [ ] Für jeden geplanten Einsatz festhalten: Welches Problem löst die KI und welche Daten fließen hinein?
- [ ] Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) um KI-Anwendungen ergänzen.
- [ ] Zusätzlich ein separates „KI-Register“ führen, um eingesetzte Tools und „Schatten-KI“ übersichtlich und strukturiert zu erfassen.

02 Personenbezogene Daten & Rechtsgrundlage

- [ ] Prüfen: Werden personenbezogene Daten verarbeitet (Namen, E-Mails, Kundendaten, Bewerbungen)?
- [ ] Für jede Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO dokumentieren (z. B. Einwilligung, Vertrag, berechtigtes Interesse).
- [ ] Datenminimierung: Nur die wirklich nötigen Daten eingeben – keine sensiblen Daten ohne klare Grundlage.
- [ ] Bei risikoreichen Verarbeitungen eine Datenschutz-Folgenabschätzung (DSFA, Art. 35 DSGVO) durchführen.
- [ ] Keine besonderen Kategorien (Gesundheit, Religion, Herkunft) in allgemeine KI-Tools eingeben.

03 Anbieter & Verträge (AVV)

- [ ] Auftragsverarbeitungsvertrag (AVV) mit dem KI-Anbieter abschließen, sobald personenbezogene Daten verarbeitet werden.
- [ ] Business-/Enterprise-Tarife nutzen: OpenAI, Anthropic, Google & Microsoft bieten dort AVVs an.
- [ ] Kostenlose Consumer-Versionen (z. B. ChatGPT Free) meiden – meist kein AVV, Daten auf US-Servern, Nutzung fürs Training.
- [ ] Prüfen, wo die Daten verarbeitet/gespeichert werden (EU-Hosting bevorzugen, z. B. Azure OpenAI mit EU-Region).
- [ ] Bei US-Anbietern – auch mit EU-Hosting – den Drittlandtransfer absichern: EU-US Data Privacy Framework (DPF) bzw. Standardvertragsklauseln prüfen.
- [ ] Sicherstellen, dass Eingaben nicht zum Training der Modelle verwendet werden (Opt-out / Vertragsklausel).

04 Tool-Auswahl & technische Sicherheit

- [ ] Zugänge personalisieren (eigene Accounts statt geteilter Logins) und Zwei-Faktor-Authentifizierung aktivieren.
- [ ] Zugriffsrechte nach Bedarf vergeben – nicht jeder braucht jedes Tool.
- [ ] Datenhistorie/Chat-Speicherung bewusst konfigurieren oder deaktivieren, wenn nicht nötig.
- [ ] Regelmäßig prüfen, welche Tools noch aktiv genutzt werden, und ungenutzte Zugänge schließen.

05 Mitarbeitende & interne Regeln

- [ ] Klare KI-Richtlinie aufsetzen: Was ist erlaubt, was nicht, welche Daten dürfen rein?
- [ ] Auf fertige „Plug-and-Play"-Vorlagen für Richtlinien & Prozesse zurückgreifen, statt das Rad neu zu erfinden.
- [ ] KI-Kompetenz schulen – seit Feb. 2025 verpflichtend nach Art. 4 EU AI Act für Unternehmen, die KI einsetzen.
- [ ] Ergebnisse immer prüfen: KI kann Fehler erfinden („Halluzinationen") – kein blindes Übernehmen.
- [ ] Ansprechperson für Fragen und Vorfälle benennen.

06 EU AI Act – das gilt ab 2026

- [ ] Verbotene Praktiken (Art. 5) sind seit 2. Februar 2025 untersagt – betroffene Anwendungen abstellen.
- [ ] Ab 2. August 2026 gelten Transparenzpflichten, Regeln für Hochrisiko-KI und die aktive Durchsetzung.
- [ ] Eingesetzte KI nach Risikoklasse einordnen (minimal / begrenzt / hoch / verboten).
- [ ] KI-generierte Inhalte gegenüber Kunden transparent kennzeichnen.

07 Laufend kontrollieren

- [ ] Einsatz und Datenflüsse mindestens jährlich überprüfen und dokumentieren.
- [ ] Bei neuen Tools die Checkliste erneut durchgehen, bevor sie produktiv gehen.
- [ ] Datenschutzvorfälle erkennen und Meldewege (72-Stunden-Frist nach Art. 33 DSGVO) bereithalten.

Unsicher, wo Sie anfangen sollen?

Im kostenlosen 30-minütigen Erstgespräch gehen wir Ihre Situation gemeinsam durch – persönlich, praxisnah, auf Deutsch. Schreiben Sie an **julia@bridgetoai.de**

Erstgespräch sichern →

Hinweis: Diese Checkliste bietet praxisorientierte Orientierung und ersetzt keine individuelle Rechtsberatung. Rechtsgrundlagen (DSGVO, EU AI Act) und Anbieterkonditionen können sich ändern – Stand: Juni 2026. Für verbindliche Auskünfte ziehen Sie bitte eine Datenschutz- bzw. Rechtsexpertin oder einen -experten hinzu.