SNSIG

DSGVO-konforme KI im Unternehmen: die Checkliste

10 Punkte, die Geschäftsführung, IT-Leitung und Datenschutz gemeinsam prüfen, bevor KI mit echten Unternehmensdaten arbeitet.

Für
Mittelstand und KMU

Zeitaufwand
ein gemeinsamer Termin

Stand
November 2026

So nutzt Du diese Checkliste

Kein Tool ist automatisch DSGVO-konform

Ob KI datenschutzkonform eingesetzt wird, hängt nicht nur vom Tool ab, sondern davon, wie Du es nutzt, welche Verträge dahinterstehen und welche Regeln im Unternehmen gelten. Die Verantwortung bleibt bei Deinem Unternehmen.

Diese Checkliste fasst die wichtigsten Punkte zusammen. Sie orientiert sich an der DSGVO, an der Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ der Datenschutzkonferenz (Mai 2024) und am EU AI Act (Verordnung (EU) 2024/1689).

In drei Schritten

- **Termin ansetzen:** Hol Geschäftsführung, IT-Leitung und Datenschutzbeauftragte:n an einen Tisch.
- **Punkt für Punkt durchgehen:** Prüffragen abhaken, Zuständigkeit und offene Aufgaben notieren.
- **Auswerten:** Die Übersicht auf der letzten Seite zeigt, wo Dein Unternehmen steht und was als Nächstes kommt.

> Diese Checkliste ersetzt keine Rechtsberatung. Für die verbindliche Bewertung Deines Einsatzszenarios ziehst Du am besten Deine:n Datenschutzbeauftragte:n hinzu.

Bereich 1: Technik und Verträge

01 Serverstandort und Datenfluss

Wo wird verarbeitet und gespeichert, und wer ist beteiligt? Verarbeitung in der EU erspart die Prüfung eines Drittlandtransfers nach Art. 44 ff. DSGVO.

- [ ] Wir wissen, wo das KI-Modell läuft und wo Chats und Dateien gespeichert werden.
- [ ] Eine Liste der Unterauftragsverarbeiter mit Standorten liegt vor.
- [ ] Bei Anbietern außerhalb der EU ist die Grundlage für den Transfer geprüft.

Zuständig: IT-Leitung _____

02 Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Sobald personenbezogene Daten in die KI gelangen, verarbeitet der Anbieter sie in Deinem Auftrag. Private Consumer-Accounts bieten in der Regel keinen AVV.

- [ ] Der AVV ist unterschrieben und abgelegt, bevor echte Daten verarbeitet werden.
- [ ] Die technischen und organisatorischen Maßnahmen (TOM) liegen vor.
- [ ] Löschfristen und Löschprozess sind geregelt.

Zuständig: Datenschutz _____

03 Kein Training mit Deinen Daten

Was in Trainingsdaten eingeflossen ist, lässt sich nicht gezielt wieder entfernen. Der Ausschluss gehört in den Vertrag, nicht nur in eine Nutzereinstellung.

- [ ] Der Vertrag schließt die Nutzung von Eingaben und Dateien zum Training aus.
- [ ] Der Ausschluss gilt für alle Nutzer:innen, ohne dass sie selbst etwas einstellen müssen.

Zuständig: Datenschutz _____

04 Zugriffsrechte und Rollen

Greift die KI auf Firmenwissen zu, etwa auf SharePoint, muss sie dieselben Berechtigungen respektieren wie Dein Dateisystem.

- [ ] Das System übernimmt bestehende Berechtigungen.
- [ ] Rollen für Admins, Fachbereiche und Nutzer:innen sind getrennt.
- [ ] Zu großzügige Freigaben in SharePoint und OneDrive sind vor dem Start bereinigt.

Zuständig: IT-Leitung _____

05 Protokollierung

Ein Audit-Log macht administrative Änderungen nachvollziehbar. Es soll Verantwortung belegen, nicht die Inhalte einzelner Chats überwachen.

- [ ] Administrative Aktionen wie Rechtevergabe und neue Wissensquellen werden protokolliert.
- [ ] Es ist geregelt, wer das Protokoll einsehen darf.

Zuständig: IT-Leitung _____

Bereich 2: Prüfung und Mitbestimmung

06 Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Pflicht bei voraussichtlich hohem Risiko für Betroffene, etwa bei der Auswertung von Bewerbungen, Leistungs- oder Gesundheitsdaten.

- [ ] Die Einsatzzwecke der KI sind beschrieben.
- [ ] Eine Schwellwertanalyse ist durchgeführt und dokumentiert.
- [ ] Falls nötig: Die DSFA ist abgeschlossen.

Zuständig: Datenschutz _____

07 Betriebsrat

Ist ein System geeignet, Verhalten oder Leistung zu überwachen, besteht ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Frühe Transparenz spart Zeit.

- [ ] Der Betriebsrat ist frühzeitig informiert.
- [ ] Es ist dokumentiert, welche Daten erfasst werden und welche nicht.
- [ ] Eine Betriebsvereinbarung oder abgestimmte Regelung liegt vor.

Zuständig: Geschäftsführung _____

Bereich 3: Organisation

08 KI-Richtlinie

Zwei verständliche Seiten wirken besser als zwanzig, die niemand liest.

- [ ] Freigegebene Tools und Zwecke sind festgelegt.
- [ ] Datenklassen sind definiert: öffentlich, intern, vertraulich, streng vertraulich.
- [ ] KI-Ergebnisse werden vor Weitergabe fachlich geprüft.
- [ ] Die Richtlinie ist veröffentlicht und allen bekannt.

Zuständig: Geschäftsführung _____

09 Schulung und KI-Kompetenz (Art. 4 AI Act)

Seit Februar 2025 verlangt der EU AI Act Maßnahmen für ausreichende KI-Kompetenz der Mitarbeitenden, die KI nutzen.

- [ ] Alle Nutzer:innen erhalten vor dem Start eine Einweisung zu Funktion, Grenzen und Risiken.
- [ ] Die Schulung ist auf die jeweilige Rolle zugeschnitten.
- [ ] Teilnahme und Inhalte sind dokumentiert.

Zuständig: HR / Geschäftsführung _____

10 Schatten-KI verhindern

Laut Bitkom (Oktober 2025) ist private KI-Nutzung in 8 % der Unternehmen weit verbreitet, in weiteren 17 % gibt es Einzelfälle. Verbote allein helfen wenig.

- [ ] Es gibt eine offiziell freigegebene KI-Lösung für alle.
- [ ] Sie deckt den tatsächlichen Bedarf der Teams ab.
- [ ] Die Nutzung wird als Kennzahl verfolgt, ohne Inhalte mitzulesen.

Zuständig: alle _____

Auswertung

Wo steht Dein Unternehmen?

Trag pro Punkt ein, ob alle Prüffragen erfüllt sind. Offene Punkte bekommen eine verantwortliche Person und ein Zieldatum.

Nr.	Punkt	Verantwortlich	Bis wann	Erledigt
01	Serverstandort und Datenfluss			☐
02	Auftragsverarbeitungsvertrag			☐
03	Kein Training mit Deinen Daten			☐
04	Zugriffsrechte und Rollen			☐
05	Protokollierung			☐
06	Datenschutz-Folgenabschätzung			☐
07	Betriebsrat			☐
08	KI-Richtlinie			☐
09	Schulung nach Art. 4 AI Act			☐
10	Schatten-KI verhindern			☐

Erfüllt	Einordnung
10 von 10	Gute Grundlage. Prüf die Punkte jährlich und bei jedem neuen Einsatzzweck erneut.
6 bis 9	Auf dem Weg. Schließ zuerst die offenen Punkte aus Bereich 1, sie betreffen jede einzelne Anfrage.
0 bis 5	Hoher Handlungsbedarf. Starte mit AVV, Trainingsausschluss und einem freigegebenen Tool.

snutig.ai

Eine KI-Plattform, die diese Checkliste mitdenkt

- KI-Modelle in EU-Rechenzentren, kein Training mit Deinen Daten, AVV nach Art. 28 DSGVO
- Jede Organisation getrennt, Rollen und Rechte, Microsoft-365-Berechtigungen bleiben erhalten
- Admins lesen keine Chats mit, betrieben von snutig aus Herford

Demo vereinbaren: snutig.de/leistungen/snutig-ai

Quellen: Datenschutzkonferenz, Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ (Mai 2024) · Verordnung (EU) 2024/1689 (AI Act), Art. 4 · Bitkom, Presseinformation „Beschäftigte nutzen vermehrt Schatten-KI“ (Oktober 2025). Diese Checkliste ersetzt keine Rechtsberatung. Microsoft 365, SharePoint und OneDrive sind Marken der Microsoft Corporation.