KI-Compliance in 5 Schritten

Diese Checkliste ermöglicht die systematische Prüfung der DSGVO-Konformität von KI-Agenten im Unternehmen und identifiziert rechtliche Risiken sowie notwendige Maßnahmen zur datenschutzkonformen Implementierung künstlicher Intelligenz.

Schritt 1: Rechtsgrundlage klären

Die Verarbeitung personenbezogener Daten durch KI-Agenten benötigt eine rechtliche Grundlage nach Art. 6 DSGVO. Unternehmen müssen prüfen, ob eine Einwilligung der betroffenen Personen erforderlich ist oder ob die Datenverarbeitung zur Vertragserfüllung, aufgrund rechtlicher Verpflichtungen oder auf Basis berechtigter Interessen erfolgt. Besonders bei sensiblen Daten nach Art. 9 DSGVO gelten verschärfte Anforderungen.

- □ Rechtsgrundlage für die KI-Datenverarbeitung dokumentiert (Art. 6 DSGVO)
- □ Bei Einwilligung: Nachweisbare, informierte und freiwillige Zustimmung eingeholt
- □ Besondere Kategorien personenbezogener Daten identifiziert (Art. 9 DSGVO)
- □ Zweckbindung der Datenverarbeitung definiert und begrenzt

Schritt 2: Transparenz sicherstellen

Betroffene Personen haben ein Recht auf Information über die KI-gestützte Verarbeitung ihrer Daten. Die Datenschutzerklärung muss verständlich erläutern, welche Daten durch welche KI-Systeme verarbeitet werden, zu welchem Zweck dies geschieht und welche automatisierten Entscheidungen getroffen werden. Bei automatisierten Einzelentscheidungen nach Art. 22 DSGVO gelten besondere Informationspflichten über die Logik und Tragweite der KI-Verarbeitung.

- □ Datenschutzerklärung enthält Informationen über KI-Einsatz
- □ Zweck und Funktionsweise der KI-Agenten verständlich beschrieben
- □ Automatisierte Entscheidungen und deren Tragweite offengelegt (Art. 22 DSGVO)
- □ Betroffenenrechte (Auskunft, Löschung, Widerspruch) implementiert

Schritt 3: Datensicherheit gewährleisten

KI-Systeme müssen durch angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO geschützt werden. Dies umfasst Verschlüsselung, Zugriffskontrolle, regelmäßige Sicherheitsupdates und Monitoring. Besonders bei Cloud-basierten KI-Diensten ist zu prüfen, wo die Datenverarbeitung stattfindet und ob Drittstaaten-Transfers erfolgen. Der KI-Anbieter muss als Auftragsverarbeiter gemäß Art. 28 DSGVO vertraglich gebunden werden, sofern personenbezogene Daten verarbeitet werden.

- □ Technische Schutzmaßnahmen implementiert (Verschlüsselung, Zugriffskontrolle)
- □ Auftragsverarbeitungsvertrag (AVV) mit KI-Anbieter abgeschlossen

□ Drittstaaten-Transfers geprüft und durch geeignete Garantien abgesichert

□ Datenschutz-Folgenabschätzung (DSFA) durchgeführt bei Hochrisiko-Verarbeitung

Schritt 4: Datenminimierung umsetzen

KI-Agenten sollten nur die Daten verarbeiten, die für den definierten Zweck tatsächlich erforderlich sind. Unnötige Datenerhebung erhöht das Risiko und widerspricht dem Grundsatz der Datenminimierung nach Art. 5 DSGVO. Trainingsdaten müssen regelmäßig überprüft werden, ob sie noch benötigt werden oder gelöscht werden können. Anonymisierung oder Pseudonymisierung sollten eingesetzt werden, wo dies möglich ist. Die Speicherdauer muss definiert und dokumentiert sein.

□ Nur erforderliche Daten werden durch KI-Agenten verarbeitet

□ Löschkonzept für Trainings- und Verarbeitungsdaten vorhanden

□ Anonymisierung oder Pseudonymisierung wo möglich eingesetzt

□ Speicherdauer festgelegt und automatisierte Löschung implementiert

Schritt 5: Compliance dokumentieren

Die DSGVO fordert eine lückenlose Dokumentation aller Verarbeitungstätigkeiten im Verzeichnis nach Art. 30 DSGVO. KI-Agenten müssen dort mit allen relevanten Details erfasst werden. Regelmäßige Audits stellen sicher, dass die KI-Systeme weiterhin datenschutzkonform betrieben werden. Schulungen sensibilisieren Mitarbeitende für den korrekten Umgang mit KI und personenbezogenen Daten. Ein Notfallplan für Datenpannen gemäß Art. 33 DSGVO muss vorbereitet sein, um im Ernstfall schnell reagieren zu können.

□ KI-Systeme im Verzeichnis von Verarbeitungstätigkeiten dokumentiert

□ Regelmäßige Datenschutz-Audits der KI-Agenten durchgeführt

□ Mitarbeiterschulungen zum datenschutzkonformen KI-Einsatz erfolgt

□ Notfallplan für Datenpannen (Art. 33 DSGVO) vorbereitet und getestet

Unterstützung bei der KI-Compliance benötigt?

Die Cortina Consult GmbH begleitet Unternehmen bei der datenschutzkonformen Implementierung von KI-Systemen. Von der rechtlichen Erstbewertung über die Datenschutz-Folgenabschätzung bis zur vollständigen DSGVO-Compliance Ihres KI-Projekts.