Datenschutz- und KI-VO-Checkliste für KI-Tools im Arbeitsalltag

Evaluative Prüfpunkte für DSGVO- und EU AI Act-Konformität

DSGVO-Compliance: Datenschutzrechtliche Prüfpunkte

Rechtsgrundlage prüfen: Ist eine Rechtsgrundlage gemäß Art. 6 DSGVO vorhanden (Einwilligung, Vertragserfüllung, berechtigtes Interesse)?

Datenminimierung sicherstellen: Werden nur die für den Zweck notwendigen Daten verarbeitet? Keine übermäßige Datensammlung? [1]

Zweckbindung beachten: Werden Daten ausschließlich für den definierten Zweck verwendet? Keine Weiterverwendung für Modelltraining ohne Einwilligung? [2]

Auftragsverarbeitungsvertrag (AVV): Liegt ein gültiger AVV gemäß Art. 28 DSGVO mit dem KI-Anbieter vor? [3]

Transparenz gewährleisten: Sind Betroffene über die KI-Nutzung und Datenverarbeitung informiert (Art. 13/14 DSGVO)? [1]

Betroffenenrechte umsetzen: Können Auskunft, Löschung, Berichtigung und Widerspruch technisch umgesetzt werden? [2]

Automatisierte Entscheidungen (Art. 22): Bei automatisierten Entscheidungen mit Rechtswirkung: Ist menschliche Überprüfung möglich? [4]

Datenschutz-Folgenabschätzung (DSFA): Ist bei Hochrisiko-Datenverarbeitung eine DSFA gemäß Art. 35 DSGVO durchgeführt? [1]

Drittlandtransfer prüfen: Werden Daten in Drittstaaten übermittelt (z.B. USA)? Sind angemessene Garantien vorhanden? [3]

Technische und organisatorische Maßnahmen (TOMs): Sind ausreichende Sicherheitsmaßnahmen implementiert (Verschlüsselung, Zugriffskontrollen, Protokollierung)? [1]

EU AI Act: Risikoklassifizierung und Compliance-Anforderungen

Risikoklasse bestimmen: In welche Kategorie fällt das KI-System (verboten, Hochrisiko, begrenztes Risiko, minimales Risiko)? [5]

Verbotene Praktiken ausschließen: Keine Social Scoring, biometrische Echtzeit-Überwachung, Emotionserkennung am Arbeitsplatz oder unterschwellige Manipulation (seit Februar 2025 verboten)? [6]

Hochrisiko-KI identifizieren: Wird KI für HR-Prozesse (Rekrutierung, Leistungsbewertung, Aufgabenzuteilung) oder Kreditentscheidungen eingesetzt (Anhang III)? [5]

Risikomanagement-System: Ist bei Hochrisiko-KI ein kontinuierliches Risikomanagementsystem gemäß Art. 9 implementiert?

Datenqualität sicherstellen: Sind Trainings- und Testdaten hochwertig, frei von Bias und ausreichend dokumentiert (Art. 10)?

Technische Dokumentation: Liegt vollständige Dokumentation über Systemdesign, Entwicklungsmethodik, Fähigkeiten und Einschränkungen vor (Art. 11, Annex IV)?

Automatische Protokollierung: Zeichnet das System automatisch Ereignisse, Eingaben, Ausgaben und Entscheidungen auf (Art. 12)? [7]

Transparenz und Kennzeichnung: Sind Nutzer darüber informiert, dass sie mit KI interagieren? Ist KI-generierter Content gekennzeichnet? [8]

Menschliche Aufsicht: Ist bei Hochrisiko-KI sinnvolle menschliche Kontrolle und Eingriffsmöglichkeit gewährleistet?

KI-Kompetenz nachweisen: Haben Mitarbeitende ausreichende KI-Literacy gemäß Art. 4 (Schulungspflicht seit Februar 2025)? [7]

Referenzen

[1] DSGVO KI Compliance: 10-Punkte-Checkliste | DigiRift

[2] DSGVO-konforme KI für Unternehmen: Checkliste & Anforderungen 2026

[3] DSGVO & KI-Verordnung Checkliste [2026] | teamazing

[4] DSGVO-konforme KI: Worauf deutsche Unternehmen achten müssen

[5] EU AI Act Compliance Checklist (2026) | Complete Step-by-Step Guide ...

[6] EU AI Act Compliance Checklist — Know Your Obligations | AAI Labs

[7] EU AI Act Compliance Checklist: 15 Steps Before August 2026

[8] EU AI Act Compliance Checker - Artificial Intelligence Act