ZEITELHACK AI · WHITEPAPER

Datenschutz & KI

DSGVO, EU AI Act & sichere Einführung im Unternehmen

Praxisleitfaden · Stand: Juni 2026
zeitelhack.ai

Über Zeitelhack AI

Zeitelhack AI begleitet mittelständische Unternehmen, Kanzleien und öffentliche Einrichtungen bei der sicheren, rechtskonformen Einführung von Künstlicher Intelligenz. Wir verbinden technische Umsetzung mit Datenschutz-Expertise und praxisnahen Schulungen – damit KI im Unternehmen nicht zum Risiko, sondern zum echten Produktivitätshebel wird.

Unsere Leistungen im KI-Bereich

KI-Strategie & Readiness-Check

Analyse Ihrer Prozesse, Identifikation sinnvoller KI-Use-Cases und Bewertung von Datenschutz- sowie AI-Act-Risiken. Ergebnis: priorisierte Roadmap mit Quick Wins.

Schulungen & Enablement

Vom Grundlagenkurs „KI für Mitarbeitende“ bis zu rollenbasierten Trainings für Führungskräfte, IT, HR und Vertrieb. Inkl. KI-Kompetenz nach Art. 4 EU AI Act.

Datenschutz & Compliance

DSFA, Auftragsverarbeitung, Risikoklassifizierung nach AI Act, interne KI-Richtlinien und Governance-Strukturen – pragmatisch und audit-fest.

Tool-Auswahl & Enterprise-Rollout

Vergleich, Pilotierung und Einführung von Microsoft 365 Copilot, ChatGPT Enterprise, Claude for Work, Gemini for Workspace sowie europäischen Alternativen.

Custom GPTs, Agenten & Automatisierung

Entwicklung maßgeschneiderter Assistenten, RAG-Lösungen auf eigenen Dokumenten und Workflow-Automatisierung – DSGVO-konform und hostbar in der EU.

Laufende Begleitung

Monatliche Sprechstunden, Updates zur Rechtslage, Review interner Prompts und kontinuierliche Optimierung Ihrer KI-Landschaft.

Kontakt: hello@zeitelhack.ai · zeitelhack.ai

Hinweis: Stand der Gesetzgebung (Digital Omnibus on AI)

Wichtig: Am 19. November 2025 hat die EU-Kommission den **Digital Omnibus on AI** vorgelegt. Am 7. Mai 2026 haben Parlament und Rat eine **vorläufige Einigung** erzielt, die zentrale Fristen des EU AI Act verschiebt:

• Hochrisiko-Pflichten für eigenständige **Anhang-III-Systeme**: verschoben auf den **2. Dezember 2027**
• Hochrisiko-KI eingebettet in **Anhang-I-Produkte**: verschoben auf den **2. August 2028**
• **Transparenz-/Kennzeichnungspflichten** nach Art. 50(2) (Watermarking): verschoben auf den **2. Dezember 2026**

Achtung: Diese Änderungen sind **noch nicht förmlich verabschiedet** und noch nicht im Amtsblatt veröffentlicht. **Solange der Omnibus nicht vor dem 2. August 2026 förmlich angenommen ist, gelten die ursprünglichen Fristen.** Kanzleien empfehlen, vorsichtshalber weiter auf den 2.8.2026 hinzuarbeiten. Die übrigen Transparenzpflichten – inklusive der Pflichten für Betreiber – gelten unverändert ab dem **2. August 2026**.

Neue inhaltliche Änderungen durch den Omnibus

Zusätzlich zu den Fristverschiebungen enthält der Digital Omnibus zwei wichtige inhaltliche Neuerungen:

- **Neue Verbotsnorm in Art. 5** gegen KI-generierte **nicht-einvernehmliche intime Bilder** („Nudifier"-Apps) sowie gegen kinderpornografisches Material (CSAM).
- **Geplante Ausnahme von der Registrierungspflicht** in der EU-Datenbank für bestimmte Hochrisiko-Systeme **ohne erhebliches Risiko**.

Inhaltsverzeichnis

1. Warum Datenschutz bei KI besonders kritisch ist

Generative KI verarbeitet in Sekunden personenbezogene Daten, Geschäftsgeheimnisse und vertrauliche Dokumente. Anders als klassische Software speichern viele KI-Dienste Eingaben standardmäßig zur Modellverbesserung – ein erhebliches Risiko für DSGVO-Verstöße, Geheimnisverletzungen und Reputationsschäden.

Die zentralen Risikofelder: unkontrollierter Datenabfluss in Public-Tools, fehlende Rechtsgrundlage nach Art. 6 DSGVO, halluzinierte Aussagen über reale Personen (Art. 5 Abs. 1 lit. d), unzulässige automatisierte Entscheidungen (Art. 22), sowie Drittlandtransfers in die USA ohne tragfähige Garantien.

2. Der EU AI Act – Risikoklassen & Zeitplan

Der AI Act (Verordnung (EU) 2024/1689) ist am 1. August 2024 in Kraft getreten und klassifiziert KI-Systeme nach Risiko:

Risikoklasse	Beispiele	Pflichten
Unzulässig	Social Scoring, manipulative KI, Nudifier/CSAM (neu, Art. 5)	Verboten
Hochrisiko	HR-Auswahl, Kreditvergabe, kritische Infrastruktur (Anhang III)	Konformität, DSFA, Registrierung
Begrenztes Risiko	Chatbots, Deepfakes, generierte Inhalte	Transparenz, Kennzeichnung
Minimales Risiko	Spamfilter, Empfehlungssysteme	Keine zusätzlichen Pflichten

Aktualisierter Zeitplan (Stand Juni 2026)

Datum	Pflicht	Status
2. Feb 2025	Verbote (Art. 5) & KI-Kompetenz (Art. 4)	In Kraft
2. Aug 2025	GPAI-Modelle, Governance, Sanktionen	In Kraft
2. Aug 2026	Allg. Anwendbarkeit, Transparenz für Betreiber (Art. 50)	In Kraft, sofern Omnibus nicht vorher beschlossen
2. Dez 2026	Watermarking/Kennzeichnung Art. 50(2) – n. Omnibus	Geplante Verschiebung
2. Dez 2027	Hochrisiko Anhang III – n. Omnibus	Geplante Verschiebung (vorher: 2.8.2026)
2. Aug 2027 / 2028	Hochrisiko Anhang I (Produktintegriert) – n. Omnibus	Verschiebung auf 2.8.2028 geplant

Quellenhinweis: Gibson Dunn, DLA Piper, Hogan Lovells, Addleshaw Goddard zum Digital Omnibus on AI (Nov 2025 / Mai 2026). Bis zur förmlichen Annahme im Amtsblatt gelten die ursprünglichen Fristen.

3. DSGVO-Compliance beim Einsatz von KI

Rechtsgrundlagen prüfen (Art. 6 DSGVO)

Jede Verarbeitung personenbezogener Daten durch KI benötigt eine Rechtsgrundlage: Vertrag (lit. b), berechtigtes Interesse (lit. f) mit Abwägung, oder Einwilligung (lit. a). Bei besonderen Kategorien (Art. 9) gelten zusätzliche Hürden.

Auftragsverarbeitung (Art. 28)

Mit jedem KI-Anbieter, der personenbezogene Daten in Ihrem Auftrag verarbeitet, ist ein AV-Vertrag erforderlich. Microsoft, OpenAI (Enterprise), Anthropic und Google stellen entsprechende Verträge sowie EU-Datenresidenz bereit.

Betroffenenrechte

Auskunft, Berichtigung, Löschung und Widerspruch müssen auch bei KI-gestützten Prozessen praktisch umsetzbar sein – inklusive trainierter Modelle und gespeicherter Chatverläufe.

4. Datenschutz-Folgenabschätzung (DSFA)

Eine DSFA nach Art. 35 DSGVO ist bei KI-Einsatz in der Regel erforderlich, insbesondere bei automatisierten Entscheidungen, systematischer Überwachung oder Verarbeitung besonderer Kategorien. Bestandteile:

- Systematische Beschreibung der Verarbeitung und Zwecke
- Bewertung der Erforderlichkeit und Verhältnismäßigkeit
- Risikobewertung für die Betroffenenrechte
- Abhilfemaßnahmen, Garantien und Sicherheitsvorkehrungen

5. Public AI vs. Enterprise

Kriterium	Public (ChatGPT Free/Plus)	Enterprise (M365 Copilot, ChatGPT Enterprise)
Training mit Eingaben	Standardmäßig ja	Nein – vertraglich ausgeschlossen
AV-Vertrag (Art. 28)	Eingeschränkt / nicht praxistauglich	Ja, mit EU-Datenresidenz
Datenresidenz	USA / global	EU-Region wählbar
SSO, Audit-Logs, DLP	Nein	Ja
Geeignet für Personenbezug	Nein	Ja, bei korrekter Konfiguration

6. Governance-Roadmap in 10 Schritten

1. Bestandsaufnahme aller eingesetzten KI-Tools (Schatten-IT inkl.)
2. Risikoklassifizierung nach EU AI Act je Use-Case
3. Interne KI-Richtlinie verabschieden und kommunizieren
4. Freigegebene Tools mit AV-Vertrag und EU-Residenz beschaffen
5. DSFA für Hochrisiko- und sensible Use-Cases erstellen
6. Schulungen zur KI-Kompetenz (Art. 4 AI Act) für alle Mitarbeitenden
7. Rollen definieren: KI-Verantwortliche, Datenschutz, IT-Sicherheit
8. Technische Schutzmaßnahmen: SSO, DLP, Logging, Pseudonymisierung
9. Lieferantenmanagement & regelmäßige Re-Assessments
10. Monitoring, Vorfallsmanagement & kontinuierliche Verbesserung

7. Technische Maßnahmen & Referenzen

Technische und organisatorische Maßnahmen (TOM)

- Single Sign-On, MFA und rollenbasierte Berechtigungen
- Data Loss Prevention (DLP) auf Prompt-Ebene
- Pseudonymisierung / Anonymisierung sensibler Eingaben
- Audit-Logs, Aufbewahrung und Löschkonzepte
- RAG-Architekturen mit Berechtigungs-Trim auf Dokumentenebene

Wichtige Referenzen

- Verordnung (EU) 2024/1689 – EU AI Act
- Digital Omnibus on AI (Kommission, Nov 2025; vorl. Einigung Mai 2026)
- DSK – Orientierungshilfe KI und Datenschutz
- EDSA – Opinion 28/2024 zu KI-Modellen
- BSI – AIC4-Kriterienkatalog für Cloud-KI

Disclaimer: Dieses Whitepaper dient der allgemeinen Information und ersetzt keine individuelle Rechtsberatung. Stand: Juni 2026. Die Rechtslage – insbesondere zum Digital Omnibus on AI – entwickelt sich dynamisch.