PERFEKTER DATENSCHUTZ

Leitfaden
KI Compliance & Implementierung

- **Risiken identifizieren** und steuern
- Rechtliche **Anforderungen erfüllen**
- **Verbindlichkeit** im Unternehmen schaffen

Nina Rümmele
TÜV zertifizierte Datenschutzbeauftrage
T: +49 69 2475 10 260
E: n.ruemmele@perfekter-datenschutz.de

TÜV SÜD

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

COMPLIANCE MADE IN GERMANY

Version 1.1
November 2025

Inhalt

1. Einleitung

Mit dem EU AI Act schafft die Europäische Union erstmals einen **verbindlichen, horizontalen Rechtsrahmen** für den Einsatz von künstlicher Intelligenz (KI) in Europa.

Für Unternehmen bedeutet das: wer KI-Systeme nutzt, entwickelt, betreibt oder in Verkehr bringt, muss frühzeitig handeln. Nicht nur, um Bußgelder oder Reputationsverluste zu vermeiden – sondern um sich langfristig im Wettbewerb vorteilhaft aufzustellen.

Dieser Leitfaden gibt Ihnen einen klaren Überblick über die Anforderungen, leitet strategische Maßnahmen ab und bietet eine praxisorientierte Checkliste zur Integration in bestehende Geschäftsmodelle.

2. Gesetzlicher Rahmen – Was ist der EU AI Act?

Der EU AI Act ist eine **Verordnung** (Regulation (EU) 2024/1689) und gilt damit unmittelbar in allen Mitgliedstaaten der EU.

Ziel ist es, ein einheitliches Niveau von Sicherheit, Transparenz, Nachvollziehbarkeit und Fundamentalrechten beim Einsatz von KI-Systemen sicherzustellen.

Wesentliche Merkmale:

- Risikobasierter Ansatz: Je höher das Risiko eines KI-Systems, desto striktere Anforderungen.
- Verbot bestimmter, als untragbar eingestufter KI-Anwendungen (z. B. Social Scoring durch staatliche Stellen)
- Verpflichtungen für Anbieter, Betreiber, Importeure und Nutzer von KI-Systemen
- Übergangs- und Stufenregelungen, damit Unternehmen sich vorbereiten können

3. Risiko- und Systemkategorien

Der Gesetzgeber differenziert zwischen verschiedenen Kategorien von KI-Systemen. Die wichtigsten im Überblick:

- **Unacceptable risk (untragbares Risiko):** Anwendungen, die fundamentale Rechte verletzen oder sehr hohe Risiken bergen sind verboten.
- **High-risk KI-Systeme:** KI-Systeme, die in sensiblen Bereichen eingesetzt werden – z.B. biometrische Identifikation, kritische Infrastruktur, Bildung, Beschäftigung, Strafverfolgung.
- **Spezifizierter geringer bis mittlerer Risikograd:** KI-Systeme mit weniger schwerwiegenden Auswirkungen (z. B. Chatbots); hier gelten Transparenz- und Kennzeichnungspflichten.
- **Minimal Risk:** KI-Systeme, die außerhalb von risikobehafteten Anwendungen liegen (z. B. reine Filterfunktionen); hier gelten kaum zusätzliche Anforderungen über bestehende Gesetze hinaus.

Für Ihr Unternehmen heißt das: **Identifizieren Sie Ihre Rolle (Anbieter vs. Betreiber) und Ihre KI-Systeme im Hinblick auf die Risiko-Kategorie**. Nur so lassen sich die richtigen Maßnahmen ableiten.

4. Anforderungen im Detail – Was müssen Unternehmen tun?

Für Unternehmen, die KI-Systeme nutzen oder bereitstellen, ergeben sich zahlreiche Anforderungen. Hier die wichtigsten im Überblick:

4.1 Verbotene Praktiken

Einige KI-Anwendungen sind grundsätzlich verboten: z. B. Social Scoring durch öffentliche oder private Stellen, subliminale Manipulation, biometrische Identifikation im öffentlichen Raum ohne Rechtsgrundlage.

4.2 Transparenzpflichten & Kennzeichnung

- KI-Systeme, die mit Menschen interagieren, müssen deutlich kenntlich machen, dass es sich um KI handelt.
- Generative KI / Sprach- und Bildmodelle müssen u.a. technische Dokumentation bereitstellen und die Datenherkunft offenlegen.

4.3 Anforderungen an High-Risk KI-Systeme

Für diese gelten umfangreiche Verpflichtungen, darunter:

- Risikomanagementsysteme (vor, während und nach dem Einsatz)
- Daten- und Daten-Governance: Trainings-, Validierungs-, Test-Datensätze müssen dokumentiert, Qualitäts- und Bias-Risiken adressiert sein.
- Technische und organisatorische Sicherheits- und Robustheitsmaßnahmen, z.B. gegen Manipulationen, Cyberangriffe
- Überwachung nach Markteinführung (Post-Market-Monitoring) und Meldung von schwerwiegenden Vorfällen.
- Menschliche Aufsicht: Der Mensch muss weiterhin in der Lage sein, Entscheidungen zu verstehen, zu überwachen und gegebenenfalls zu intervenieren.
- Registrierungspflicht: Vor Markt- oder Dienstleistungsbeginn muss das System ggf. in einem EU-Register gemeldet werden.

4.4 Rollen: Anbieter vs. Betreiber

- **Anbieter (Provider):** Wer ein KI-System entwickelt oder in Verkehr bringt.
- **Betreiber (Deployers/User):** Wer ein KI-System nutzt oder betreibt.

Ein Unternehmen kann beide Rollen innehaben – etwa wenn eigene KI-Lösungen weiterentwickelt oder verkauft werden.

4.5 Weitere Verpflichtungen

- Sicherstellung der **KI-Kompetenz/Ausbildung** von Mitarbeitenden („AI-Literacy“)
- Marktüberwachung, Meldepflichten, Behördenzugriff auf Unterlagen.
- Sanktionen: Verstöße können erhebliche Bußgelder bedeuten (bis zu 35 Mio € oder 7 % des weltweiten Jahresumsatzes).

---

5. Zeitplan & Meilensteine

Damit Sie wissen, wann Sie welchen Umsetzungsgrad erreichen müssen, hier der zentrale Zeitplan der KI Verordnung:

Datum	Meilenstein
12. Juli 2024	Veröffentlichung im Amtsblatt der EU.
1. August 2024	Inkrafttreten der Verordnung.
2. Februar 2025	Erste Verbote untragbarer KI-Systeme gelten.
2. August 2025	Verpflichtungen für GPAI-Anbieter, Governance, Melde- und Verwaltungsstrukturen.
2. August 2026	Breiter Einsatz: viele Anforderungen für High-Risk-KI-Systeme (Annex III) greifen.
2. August 2027	Vollständige Anwendung auch für High-Risk-KI-Systeme, die eingebettet sind bzw. Produkte darstellen.

6. Umsetzungsschritte – Strategie für Unternehmen

Nachfolgende strukturierte Vorgehensweise hilft Ihnen, die wesentlichen Schritte konkret anzugehen:

Schritt 1: Inventarisierung

- Erfassen Sie **alle KI-Systeme** im Einsatz: Eigenentwicklung, gekaufte Lösungen, KI-Komponenten in Produkten.
- Klären Sie Rolle: Anbieter oder Betreiber oder beides.
- Klassifizieren Sie jedes System nach Risikokategorie (Unacceptable / High-Risk / Sonstige).

Schritt 2: Risikoanalyse & Gap-Analyse

- Für jedes System insbesondere High-Risk: Welche Risiken bestehen für Sicherheit, Grundrechte, Transparenz?
- Prüfen Sie bestehende Dokumentation, Datenqualität, Nutzerinformation, Überwachungs- und Kontrollmechanismen.
- Identifizieren Sie Lücken gegenüber den Anforderungen des Gesetzes.

Schritt 3: Maßnahmenplan & Governance-Struktur

- Verantwortlichkeiten definieren: Wer im Unternehmen ist „KI-Compliance Verantwortlicher“?
- Governance-Strukturen aufbauen: KI-Richtlinien, Compliance-Handbuch, Meldeprozesse für Vorfälle.
- Schulungsprogramme (AI-Literacy) für Mitarbeitende einführen.

Schritt 4: Technische und organisatorische Maßnahmen umsetzen

- Daten-Governance etablieren: Dokumentation von Trainings-, Validierungs-, Testdaten; Bias-Analyse.
- Robustheit und Sicherheit: Modelle gegen Manipulation absichern, Monitoring einrichten.
- Menschliche Aufsicht sicherstellen.
- Transparenz schaffen: Nutzer informieren, KI-Interaktionen kennzeichnen.
- Registrierung – sofern erforderlich – bei zuständigen Behörden / EU-Register.

Schritt 5: Monitoring, Reporting & kontinuierliche Verbesserung

- Nach Markteinführung: Post-Market-Monitoring einrichten (Performance, Bias, unerwünschte Nebenwirkungen).
- Vorfälle / Zwischenfälle melden.
- Compliance-Berichte produzieren, Auditierung vorbereiten.
- Prozesse regelmäßig prüfen und anpassen (z. B. wenn neues KI-System eingeführt wird oder Gesetzgebung sich weiterentwickelt).

Schritt 6: Kommunikation & Marktpositionierung

- Kommunikation nach außen: Ihr Unternehmen positioniert sich als verantwortungsbewusster Anbieter/Nutzer von KI.
- Wettbewerbsvorteil erzeugen durch Compliance und Transparenz.
- Angebote entsprechend anpassen (z. B. vertrauenswürdige KI-Lösungen als USP).

7. Checkliste & Cheat-Sheet für KI-Compliance

Checkliste – Ihr Fahrplan

- O Alle KI-Systeme erfasst und klassifiziert
- O Rolle („Anbieter“ vs. „Betreiber“) bestätigt
- O Risiko- und Gap-Analyse durchgeführt
- O Governance-Struktur & Verantwortlichkeiten definiert
- O Daten-Governance eingeführt (Trainings-, Validierungs-, Testdaten)
- O Technische & organisatorische Schutz- und Monitoring-maßnahmen implementiert
- O Transparenz- und Kennzeichnungspflichten erfüllt (z. B. Nutzer-Hinweise)
- O Registrierungspflichten geprüft und ggf. erfüllt
- O Post-Market-Monitoring eingerichtet
- O Mitarbeitende geschult (AI-Literacy)
- O Kommunikations- und Marketingstrategie zur verantwortungsvollen KI positioniert

Cheat-Sheet – Kurzform

- **„Was?“** → Regulation (EU) 2024/1689 – erster horizontaler AI-Regelungsrahmen.
- **„Wer?“** → Anbieter, Betreiber, Importeure, Nutzer.
- **„Welche Systeme?“** → Unacceptable (verboten) / High-Risk / Sonstige.
- **„Wann?“** → Inkraft 1.8.2024; erste Verbote 2.2.2025; High-Risk Standards ab 2.8.2026; volle Wirkung ggf. 2.8.2027.
- **„Was muss ich tun?“** → Inventar, Risikoanalyse, Maßnahmenplan, Daten- & Sicherheitsmaßnahmen, Monitoring, Schulung.
- **„Was riskiere ich?“** → Bußgelder bis zu 7 % des weltweiten Jahresumsatzes + Reputationsschäden.

8. Best Practices & Integrationsstrategien

- **Früh starten:** Der Vorteil für Sie liegt darin, Compliance frühzeitig als Wettbewerbsvorteil zu nutzen. Unternehmen, die noch warten, riskieren regulatorische Rückstände.
- **Modular denken:** Beginnen Sie mit den kritischsten Systemen (High-Risk) – setzen Sie dort prioritäre Maßnahmen.
- **Interdisziplinär arbeiten:** Datenschutz, IT-Sicherheit, Geschäftsführung, Compliance – alle müssen mit an Bord sein.
- **Dokumentation automatisieren:** Nutzen Sie Tools und Vorlagen, um Daten-Governance, Monitoring, Aufsicht nachzuverfolgen.
- **Kommunikation intern & extern:** Mitarbeitende müssen verstehen, warum die Maßnahmen nötig sind; nach außen kann Compliance Vertrauen schaffen.
- **Kontinuierliche Überprüfung:** Gesetzgebung, Technik und Markt verändern sich schnell – Ihre Prozesse müssen agil bleiben.

9. Risikofolgen bei Nicht-Compliance

- Hohe Bußgelder: bis zu **35 Mio. € oder 7 % des weltweiten Jahresumsatzes** bei großem Unternehmen.
- Reputationsschäden: Verbraucher und Geschäftspartner erwarten zunehmend verantwortungsvollen KI-Einsatz.
- Markt- und Wettbewerbsnachteil: Wer Compliance nicht als Chance nutzt, fällt zurück.
- Haftungs- und Prozessrisiken: Fehlende Dokumentation, mangelhafte Aufsicht oder fehlerhafte Systeme können Schaden verursachen.
- Risiko, außen vor zu bleiben: auf Auftrags- oder Ausschreibungsseite kann Compliance zur Voraussetzung werden.

10. Fazit & Handlungsempfehlung

Für Sie als Geschäftsführer / Führungskraft gilt: Der EU AI Act ist **nicht nur ein weiteres "Regulierungs-Ding"** — er ist eine Chance, KI-Einsatz verlässlich, vertrauenswürdig und zukunftssicher zu gestalten.

Nutzen Sie diesen Leitfaden, um systematisch und strategisch vorzugehen:

- Vetonen Sie nicht – initiieren Sie.
- Strukturieren Sie Ihre KI-Landschaft konsequent.
- Setzen Sie klare Verantwortlichkeiten, Prozesse und Dokumentationen.
- Machen Sie Compliance zu einem Wettbewerbsvorteil.

Wenn Sie diese Schritte ernst nehmen und zeitnah starten, sind Sie nicht nur auf der sicheren Seite – Sie setzen ein Zeichen, das Kunden und Partner wahrnehmen werden. Gerne unterstützen wir Sie auf diesem Weg.