AiNJA

Whitepaper

EU AI Act – Governance Framework

Strukturierte Umsetzungspflichten für Unternehmen

1. Einordnung: Warum der EU AI Act kein „IT-Thema“ ist

Mit Inkrafttreten der Verordnung (EU) 2024/1689 (AI Act) ist Künstliche Intelligenz erstmals umfassend reguliert. Anders als frühere Digitalregulierungen adressiert der AI Act nicht einzelne Branchen, sondern technologiebezogene Risiken.

Für Unternehmen bedeutet dies:

- KI ist kein isoliertes Innovationsthema mehr.
- KI ist kein reines Compliance-Thema.
- KI ist eine Governance-Frage auf Managementebene.

Der AI Act wirkt horizontal. Er betrifft Anbieter, Betreiber („Deployers“), Importeure und Händler von KI-Systemen. Je nach Rolle entstehen unterschiedliche Pflichten – insbesondere im Bereich Risikobewertung, Transparenz, Dokumentation und organisatorischer Kontrolle.

Unternehmen, die generative KI einsetzen oder entwickeln, müssen ihre Strukturen systematisch anpassen.

2. Risikobasierter Ansatz: Die Architektur des AI Act

Der AI Act folgt einem vierstufigen Risikomodell:

1. **Unzulässige KI-Systeme**
2. **Hochrisiko-Systeme**
3. **Transparenzpflichtige Systeme**
4. **Systeme mit minimalem Risiko**

Für Unternehmen entscheidend ist die korrekte Einordnung:

- Wird ein KI-System intern eingesetzt?
- Wird es am Markt bereitgestellt?
- Verarbeitet es personenbezogene Daten?
- Beeinflusst es Zugang zu Arbeit, Bildung, Krediten oder öffentlichen Leistungen?

Die Klassifizierung entscheidet über:

- Konformitätsbewertung
- Dokumentationspflichten
- Risikomanagementsysteme
- Überwachungspflichten
- Haftungsrisiken

Fehleinordnungen können erhebliche Bußgelder nach sich ziehen.

3. Zentrale Umsetzungspflichten für Unternehmen

3.1 Governance-Struktur

Unternehmen benötigen eine klar definierte Verantwortungsstruktur für KI-Systeme:

- Benennung interner Zuständigkeiten
- Dokumentierte Entscheidungsprozesse
- Eskalationsmechanismen bei Risiken
- Integration in bestehende Compliance-Strukturen

Der AI Act verlangt faktisch eine institutionalisierte KI-Governance.

3.2 Risikomanagement

Für Hochrisiko-Systeme ist ein fortlaufendes Risikomanagementsystem vorgeschrieben. Dieses umfasst:

- Risikoidentifikation
- Risikoanalyse
- Risikominderung
- Monitoring und Dokumentation

Unternehmen müssen nachweisen können, dass Risiken aktiv gesteuert werden – nicht nur bei Markteinführung, sondern während des gesamten Lebenszyklus.

3.3 Technische Dokumentation

Anbieter und teilweise auch Betreiber müssen technische Dokumentation vorhalten, u.a.:

- Systembeschreibung
- Trainingsdatenbeschreibung
- Performance-Metriken
- Sicherheitsmaßnahmen
- Protokollierung

Diese Dokumentation dient der Nachvollziehbarkeit gegenüber Behörden.

Fehlende oder unvollständige Dokumentation ist ein unmittelbares Sanktionsrisiko.

3.4 Transparenzpflichten

Bestimmte KI-Systeme unterliegen Transparenzanforderungen, insbesondere:

- Kennzeichnung von KI-generierten Inhalten
- Offenlegung automatisierter Interaktion
- Hinweise bei Emotionserkennung

Gerade bei generativen Systemen (Text, Bild, Audio) entstehen neue Offenlegungspflichten.

Unternehmen müssen interne Richtlinien entwickeln, wann und wie Kennzeichnung erfolgt.

3.5 Überwachung nach Inverkehrbringen

Für Anbieter besteht eine Pflicht zur Marktüberwachung und zur Meldung schwerwiegender Vorfälle.

Das bedeutet:

- Monitoring-Strukturen
- Incident-Reporting-Prozesse
- Dokumentierte Reaktionsmechanismen

AI-Compliance endet nicht mit dem Produktlaunch.

4. Schnittstellen zu anderen Rechtsbereichen

Der AI Act wirkt nicht isoliert.

Er interagiert insbesondere mit:

- DSGVO
- Produkthaftungsrecht
- Urheberrecht
- Wettbewerbsrecht
- IT-Sicherheitsrecht

Unternehmen müssen daher interdisziplinär denken.

Beispiel:

Ein generatives KI-System kann gleichzeitig
– datenschutzrechtliche Fragen
– urheberrechtliche Fragen

– Transparenzpflichten nach AI Act
– haftungsrechtliche Risiken

auslösen.

Eine fragmentierte Betrachtung führt zu Lücken.

5. Organisatorische Verankerung: Das Governance-Modell

Ein belastbares AI-Act-Governance-Modell umfasst:

- KI-Register im Unternehmen
- Klassifizierungsverfahren für neue Systeme
- Freigabeprozesse
- Dokumentationsstandards
- Schulungen
- interne Kontrollmechanismen
- regelmäßige Auditierung

AI-Compliance muss in bestehende Compliance-, Risk- und Audit-Strukturen integriert werden.

Ad-hoc-Lösungen sind langfristig nicht tragfähig.

6. Management-Perspektive

Der AI Act ist kein Innovationshemmnis.

Er ist ein Strukturierungsinstrument.

Unternehmen, die frühzeitig:

- klare Prozesse
- dokumentierte Entscheidungen
- Governance-Strukturen
- Transparenzmechanismen

implementieren, reduzieren nicht nur Bußgeldrisiken, sondern auch Reputations- und Litigation-Risiken.

7. Fazit

Der EU AI Act verschiebt KI von einer experimentellen Technologie in einen regulierten Unternehmensbereich.

Unternehmen benötigen:

- strukturelle Verantwortlichkeit
- risikobasierte Klassifizierung
- technische und organisatorische Dokumentation
- integrierte Governance-Modelle

AI-Compliance ist kein Einmalprojekt.
Sie ist ein fortlaufender Organisationsprozess.

Dr. Anja M. Neubauer berät Unternehmen im deutschsprachigen Raum zur Entwicklung belastbarer KI-Governance-Architekturen sowie zur rechtssicheren Absicherung menschlicher Originalität im Kontext generativer Systeme.

Version 1.0 – Stand: Februar 2026