WHITEPAPER

EU AI ACT FÜR UNTERNEHMEN

Technischer und regulatorischer Leitfaden für rechtssichere KI Nutzung

Künstliche Intelligenz ist längst Teil moderner Unternehmensprozesse. Sie unterstützt bei Texten, Analysen, Kundenkommunikation, Prozessautomatisierung, Dokumentenprüfung, Reporting und Softwareentwicklung. Gleichzeitig entstehen neue Risiken durch unklare Verantwortlichkeiten, ungeprüfte Datenverarbeitung, fehlende Transparenz und unkontrollierte Tool Nutzung.

Der EU AI Act schafft erstmals einen verbindlichen europäischen Rechtsrahmen für künstliche Intelligenz. Unternehmen müssen künftig wissen, welche KI Systeme sie einsetzen, welche Risiken daraus entstehen und welche organisatorischen, rechtlichen und technischen Pflichten zu erfüllen sind. Dieses Whitepaper zeigt, wie Unternehmen ihre KI Nutzung strukturiert erfassen, bewerten und in ein belastbares Governance Modell überführen können.

WHITEPAPER

Warum KI Governance zur Führungsaufgabe wird

Autor: Hakan Cobanoglu

Die neue regulatorische Realität

Der EU AI Act ist am 1. August 2024 in Kraft getreten. Erste Pflichten gelten bereits seit dem 2. Februar 2025, insbesondere das Verbot bestimmter KI Praktiken und Anforderungen an KI Kompetenz. Weitere Pflichten folgen stufenweise und betreffen Unternehmen je nach Rolle, Einsatzbereich und Risikoklasse der verwendeten KI Systeme.

Für Unternehmen bedeutet das: KI darf nicht mehr nur technisch eingeführt oder durch einzelne Fachbereiche genutzt werden. Der Einsatz von KI muss nachvollziehbar, dokumentiert und kontrollierbar sein. Entscheidend ist nicht allein, welches Tool eingesetzt wird, sondern wofür es genutzt wird, welche Daten verarbeitet werden und ob daraus rechtliche, technische oder organisatorische Risiken entstehen.

Besonders relevant wird dies dort, wo KI in sensiblen Bereichen eingesetzt wird, etwa im Personalwesen, in Kundenprozessen, im Finanzbereich, in Compliance, IT Sicherheit, Produktion, Logistik oder bei geschäftskritischen Entscheidungen. Gerade dort entstehen Anforderungen an Transparenz, Verantwortlichkeit, Prüfung und laufende Kontrolle.

Der EU AI Act ist damit kein isoliertes Rechtsthema. Er betrifft Geschäftsführung, IT, Datenschutz, Compliance, Fachbereiche und operative Prozesse gleichermaßen. Unternehmen müssen deshalb frühzeitig klären, wer KI Anwendungen freigibt, wer Risiken bewertet, wer die Nutzung überwacht und wie Entscheidungen dokumentiert werden.

Ohne diese Struktur entsteht schnell eine Lücke zwischen technischer Nutzung und regulatorischer Verantwortung. Unternehmen sollten deshalb nicht warten, bis einzelne KI Anwendungen problematisch werden, sondern ihre Nutzung frühzeitig erfassen, bewerten und in klare Governance Prozesse überführen.

Warum viele Unternehmen noch nicht vorbereitet sind

In vielen Unternehmen wird KI bereits genutzt, ohne dass eine vollständige Übersicht besteht. Mitarbeitende verwenden externe KI Tools, Fachbereiche testen neue Lösungen, Softwareanbieter integrieren KI Funktionen und Plattformen wie Microsoft 365, CRM oder ERP Systeme erweitern ihre Anwendungen zunehmend um KI.

Das Problem liegt selten in fehlender Absicht, sondern in fehlender Transparenz. Unternehmen wissen häufig nicht vollständig, welche KI Systeme im Einsatz sind, welche Daten verarbeitet werden, wer verantwortlich ist und ob regulatorische Pflichten entstehen.

Ohne ein strukturiertes KI Inventar, eine Risikoklassifizierung und klare Governance Prozesse entsteht ein Umfeld, in dem rechtliche, technische und organisatorische Risiken zu spät erkannt werden.

Die Risikologik des EU AI Acts

Die Risikologik des EU AI Acts
Der EU AI Act reguliert KI nicht pauschal, sondern risikobasiert. Entscheidend ist nicht nur, ob ein Unternehmen KI nutzt, sondern wofür die KI eingesetzt wird, welche Daten verarbeitet werden und welche Auswirkungen das System auf Menschen, Entscheidungen oder Geschäftsprozesse haben kann.

Damit verschiebt sich der Fokus von der reinen Tool Auswahl hin zur konkreten Nutzung im Unternehmen. Ein KI System kann in einem Bereich unterstützend und risikoarm sein, in einem anderen Bereich aber erhebliche Anforderungen auslösen, etwa wenn personenbezogene Daten, Bewertungen oder automatisierte Entscheidungsvorbereitungen betroffen sind.

Was Unternehmen daraus ableiten müssen

Unternehmen müssen ihre KI Anwendungen nicht nur erfassen, sondern systematisch bewerten. Ein KI Tool im Marketing kann weitgehend unkritisch sein, während ein vergleichbares System im Recruiting, in der Leistungsbewertung oder bei geschäftskritischen Entscheidungen deutlich höhere regulatorische Anforderungen auslösen kann.

Entscheidend ist deshalb nicht allein die Technologie, sondern der konkrete Einsatzzweck. Unternehmen müssen nachvollziehen können, welche Daten verarbeitet werden, ob personenbezogene Informationen betroffen sind, wie nah das System an Entscheidungen heranrückt und welche Folgen für Mitarbeitende, Kunden oder Dritte entstehen können.

Dafür braucht es einen strukturierten Bewertungsprozess. Dieser Prozess sollte Zweck, Datenbasis, Entscheidungsnähe, Betroffenheit von Personen, Anbieterrolle, Betreiberpflichten, Transparenzanforderungen und technische Kontrollierbarkeit berücksichtigen.

Besonders problematisch wird es dort, wo KI Systeme ohne zentrale Steuerung eingeführt werden. Fachbereiche testen eigenständig neue Lösungen, Mitarbeitende nutzen externe KI Dienste und bestehende Plattformen erweitern ihre Funktionen zunehmend um generative KI.

Dadurch entstehen Risiken häufig nicht durch böse Absicht, sondern durch fehlende Übersicht. Genau deshalb brauchen Unternehmen einen verbindlichen Prozess, der neue KI Anwendungen vor der Nutzung prüft, Verantwortlichkeiten festlegt und dokumentiert, warum ein System erlaubt, eingeschränkt oder nicht freigegeben wird.

Nicht jedes KI System ist Hochrisiko.
Aber jedes KI System braucht eine bewusste Entscheidung, ob und wie es eingesetzt werden darf.

WHITEPAPER

Vom KI Inventar zur umsetzbaren Governance

Ein wirksames KI Governance Modell beginnt nicht mit einer einzelnen Richtlinie, sondern mit einem strukturierten Prozess. Unternehmen müssen KI Anwendungen erfassen, Risiken bewerten, Verantwortlichkeiten festlegen und Nachweise nachvollziehbar dokumentieren.

Eine einzelne KI Richtlinie reicht in der Praxis nicht aus. Entscheidend ist, dass Governance im Unternehmensalltag tatsächlich funktioniert. Fachbereiche müssen verstehen, welche KI Anwendungen zulässig sind, welche Daten nicht verarbeitet werden dürfen, wann eine Freigabe erforderlich ist und wie Risiken dokumentiert oder eskaliert werden.

Gleichzeitig müssen technische Umsetzung, Datenschutz, Informationssicherheit und organisatorische Verantwortung zusammengeführt werden. KI Compliance entsteht nicht durch einzelne Dokumente, sondern durch belastbare Prozesse, klare Zuständigkeiten und nachvollziehbare Entscheidungen.

Besonders wichtig ist dabei die Verbindung zwischen Management, IT, Datenschutz, Compliance und operativen Fachbereichen. Nur wenn diese Bereiche zusammenarbeiten, können KI Anwendungen kontrollierbar, transparent und langfristig verantwortungsvoll betrieben werden.

Unternehmen benötigen deshalb nicht nur Regeln, sondern ein dauerhaft tragfähiges Governance Modell, das neue KI Systeme, regulatorische Anforderungen und technische Entwicklungen kontinuierlich berücksichtigen kann.

WHITEPAPER

Was Unternehmen jetzt konkret tun sollten

KI Inventar als Ausgangspunkt

Der erste Schritt ist ein vollständiges und belastbares KI Inventar. Es erfasst bestehende und geplante KI Anwendungen, beteiligte Fachbereiche, eingesetzte Anbieter, Datenquellen, Zwecke, Nutzergruppen und interne Verantwortlichkeiten.

Viele Unternehmen unterschätzen, wie viele KI Funktionen bereits heute unbemerkt im Einsatz sind. Neben eigenständig eingeführten Tools integrieren auch Standardplattformen wie Microsoft 365, CRM, ERP oder Collaboration Systeme zunehmend generative KI Funktionen in bestehende Prozesse.

Ohne ein strukturiertes Inventar kann ein Unternehmen nicht nachvollziehbar bewerten, ob eine KI Anwendung unkritisch, transparenzpflichtig, hochrisikonah oder vertieft prüfungsbedürftig ist. Ein KI Inventar ist deshalb kein einmaliges Dokument, sondern Bestandteil einer laufenden Governance Struktur. Es muss kontinuierlich gepflegt werden, sobald neue Tools, Funktionen oder Einsatzbereiche hinzukommen.

Risikoklassifizierung nach EU AI Act

Der EU AI Act folgt einem risikobasierten Ansatz. Entscheidend ist nicht nur, ob KI genutzt wird, sondern wofür sie eingesetzt wird und welche Auswirkungen sie auf Menschen, Entscheidungen oder Geschäftsprozesse haben kann.

Unternehmen sollten jede KI Anwendung nach Zweck, Datenbasis, Entscheidungsnähe, Betroffenheit von Personen, Transparenzpflichten und möglicher Hochrisiko Nähe bewerten.

Governance, Datenschutz und IT Umsetzung verbinden

Eine reine KI Policy reicht nicht aus. Unternehmen benötigen klare Rollen, nachvollziehbare Freigabeprozesse, Schulungen, Kontrollmechanismen und technische Schutzmaßnahmen, um KI Anwendungen dauerhaft sicher und kontrollierbar betreiben zu können.

Gleichzeitig müssen Datenschutz, Informationssicherheit, Berechtigungskonzepte, Datenqualität, Systemintegration und Dokumentationspflichten berücksichtigt werden. KI Compliance funktioniert nur dann nachhaltig, wenn rechtliche Anforderungen und technische Realität miteinander verbunden werden.

Besonders kritisch wird dies dort, wo KI Entscheidungen Einfluss auf Mitarbeitende, Kunden, Bewerbungen, Bewertungen oder geschäftskritische Prozesse haben können. Unternehmen benötigen deshalb nachvollziehbare Verantwortlichkeiten und belastbare Kontrollmechanismen.

Quteco betrachtet den EU AI Act nicht isoliert als Rechtsthema. Wir verbinden regulatorische Einordnung, Datenschutz, IT Beratung, Prozessverständnis und operative Umsetzung zu einem strukturierten Governance Ansatz.

Handlungsimpuls für Unternehmen

Unternehmen sollten jetzt mit drei Fragen beginnen:

- Welche KI Systeme nutzen wir heute bereits?
- Welche davon können rechtlich, technisch oder organisatorisch kritisch sein?
- Und verfügen wir über einen dokumentierten Prozess, um KI Anwendungen nachvollziehbar zu prüfen, freizugeben und laufend zu kontrollieren?

Wenn diese Fragen nicht klar beantwortet werden können, ist ein strukturierter EU AI Act Quick Check der nächste sinnvolle Schritt.

Hakan Cobanoglu begleitet Unternehmen bei der strukturierten Umsetzung digitaler Transformationsprojekte mit Schwerpunkt auf Prozessstabilität, Governance, Qualitätsmanagement und technischer Umsetzbarkeit.