Regulatorische Entwicklungen

Weitere regulatorische Entwicklungen

Letztes Update: Oktober 2024

pwc

Inhaltsverzeichnis

1 Rechtliche Entwicklungen

1.1 EU-Verordnung über künstliche Intelligenz (EU-KI-Verordnung, EU AI Act)

Die EU-KI-Verordnung führt einen risikobasierten Rahmen für die Regulierung von Systemen künstlicher Intelligenz ein. Diese Verordnung legt die Regeln für die Entwicklung, das Inverkehrbringen und die Nutzung von KI-Systemen in der Europäischen Union fest und soll sicherstellen, dass KI vertrauenswürdig und ethisch ist und die Grundrechte respektiert.

Status: In Kraft seit 1. August 2024

Anwendbarkeit von strikten Bestimmungen zur künstlichen Intelligenz

Die EU-KI-Verordnung, welche am 1. August 2024 in Kraft trat, führt einen neuen Rechtsrahmen für die Regelung von Systemen künstlicher Intelligenz ein. Sie legt Regeln für die Entwicklung, das Inverkehrbringen und die Nutzung von KI in der Europäischen Union fest.

Die EU-KI-Verordnung gilt sowohl für Anbieter und Nutzer von KI-Systemen, die innerhalb der EU tätig sind, als auch für Anbieter und Nutzer ausserhalb der EU, wenn die vom KI-System erzeugten Ergebnisse in der EU verwendet werden sollen. Dieser extraterritoriale Geltungsbereich bedeutet, dass Unternehmen und Organisationen, einschliesslich Schweizer Unternehmen, die EU-KI-Verordnung einhalten müssen, wenn ihre KI-Systeme Auswirkungen auf EU-Bürger haben.

Compliance

Die EU-KI-Verordnung legt einen risikobasierten Ansatz für KI-Systeme fest, der auf den potenziellen Risiken basiert, die sie für die Grundrechte, die Sicherheit und die Privatsphäre darstellen. Die EU-KI-Verordnung unterteilt KI-Systeme in vier Hauptkategorien, basierend auf dem Grad des Risikos, das sie darstellen: unannehmbares, hohes, begrenztes und geringstes Risiko.

Systeme in der Kategorie „**unannehmbares Risiko**“, die eine erhebliche Bedrohung für die Sicherheit, die Rechte oder die Demokratie darstellen (z. B. KI-System für ein soziales Punktesystem durch die Regierungen), sind verboten. Systeme mit **hohem Risiko**, die in kritischen Sektoren wie dem Gesundheitswesen, der Strafverfolgung und dem Transportwesen eingesetzt werden, unterliegen strengen Anforderungen, einschliesslich Risikobewertungen, Datenverwaltung und menschlicher Aufsicht. Diese Systeme müssen ebenfalls in einer EU-Datenbank für hochriskante KI-Systeme registriert werden.

KI-Systeme **mit begrenztem Risiko**, wie sie beispielsweise bei Chatbot-Interaktionen zum Einsatz kommen, erfordern Transparenzverpflichtungen, während KI-Systeme mit **geringstem Risiko** weitgehend unreguliert sind.

Die EU-KI-Verordnung führt mehrere Compliance-Anforderungen ein, wie z. B. die Verpflichtung, die menschliche Aufsicht über KI-Systeme sicherzustellen, eine genaue Datendokumentation und robuste Risikomanagementprozesse. Organisationen, die KI-Systeme entwickeln oder einsetzen, müssen ausserdem Konformitätsbewertungen für Systeme mit hohem Risiko durchführen und in bestimmten Fällen Selbstbewertungen für Anwendungen mit geringerem Risiko vornehmen. Das Europäische Amt für künstliche Intelligenz wird die Durchsetzung überwachen und sowohl nationalen Behörden als auch Unternehmen Orientierungshilfen bieten. Bei Nichteinhaltung werden erhebliche Strafen verhängt. Verstösse gegen die EU-KI-Verordnung, insbesondere solche, die hochriskante

oder verbotene KI-Systeme betreffen, können zu Geldbussen von bis zu 6 % des weltweiten Jahresumsatzes oder EUR 30 Millionen führen, je nachdem, welcher Betrag höher ist. Dies verdeutlicht die schwerwiegenden finanziellen Risiken für Unternehmen, welche sich nicht an die Verordnung halten.

Die EU-KI-Verordnung zielt darauf ab, Innovation und öffentliches Vertrauen in Einklang zu bringen, indem sichergestellt wird, dass KI-Systeme so konzipiert, entwickelt und eingesetzt werden, dass die Grundrechte und -freiheiten des Einzelnen geschützt werden. Diese Verordnung wird wahrscheinlich tiefgreifende Auswirkungen auf die KI-Innovation in ganz Europa haben, insbesondere für Unternehmen, die in Sektoren mit hoher regulatorischer Kontrolle oder Verbraucherinteraktion tätig sind. Die EU-KI-Verordnung betont auch die KI-Governance und fordert Transparenz und Nachvollziehbarkeit bei der Entscheidungsfindung im Bereich KI, was von den Unternehmen erhebliche technische und organisatorische Anstrengungen zur Gewährleistung der Einhaltung der Vorschriften erfordert.

Ähnlich wie die EU-DSGVO (Datenschutz-Grundverordnung) stellt auch die EU-KI-Verordnung einen entscheidenden Wandel in den Regulierungsansätzen dar, indem sie die transformative Kraft der KI anerkennt und gleichzeitig die Risiken für den Einzelnen und die Gesellschaft als Ganzes anspricht. Der Fokus auf Verantwortlichkeit, Fairness und Transparenz findet in verschiedenen Sektoren Anklang, und Unternehmen müssen ihre KI-Governance-Modelle entsprechend anpassen, um die Einhaltung der Vorschriften aufrechtzuerhalten.

Wer ist betroffen?

Jede Organisation, die KI innerhalb der Europäischen Union entwickelt oder einsetzt, unterliegt der EU-KI-Verordnung. Dies schliesst auch Nicht-EU-Organisationen ein, die KI-basierte Dienstleistungen oder Produkte für EU-Bürger anbieten oder innerhalb der EU tätig sind. So muss beispielsweise ein Schweizer Technologieunternehmen, das KI-gesteuerte medizinische Diagnosesoftware in der EU einsetzt, die Regeln der EU-KI-Verordnung für Anwendungen mit hohem Risiko einhalten.

Was ist zu tun?

Um auf die EU-KI-Verordnung vorbereitet zu sein, empfehlen wir folgende nächste Schritte:

- Analysieren Sie KI-Systeme, die derzeit in Betrieb oder in Planung sind, und identifizieren Sie jene KI-Systeme mit hohem oder begrenztem Risiko innerhalb Ihrer Betriebsabläufe, die den neuen Vorschriften unterliegen werden.
- Stellen Sie sicher, dass Ihre KI-Entwicklungsprozesse von Anfang an Risikomanagement, Tests und Transparenz integrieren.
- Überprüfen Sie Ihre Dokumentation und Risikobewertungsprotokolle, um sie an die Standards der EU-KI-Verordnung anzupassen, insbesondere bei Systemen mit hohem Risiko.

Ihre PwC-Expertinnen und -Experten für KI und Datenschutz können Sie bei der Bewertung Ihrer aktuellen KI-Systeme unterstützen, Sie durch das regulatorische Umfeld führen und sicherstellen, dass Sie die neue EU-KI-Verordnung einhalten.

1.2 EU-Datenverordnung (EU Data Act)

Die EU-Datenverordnung zielt darauf ab, einen harmonisierten Rahmen für den Austausch, den Zugang und die Nutzung von Daten zwischen Unternehmen, Verbrauchern und öffentlichen Einrichtungen in der gesamten Europäischen Union zu schaffen. Die Datenverordnung legt den Schwerpunkt auf nicht personenbezogene Daten und stellt sicher, dass datengesteuerte Innovationen gefördert werden, während gleichzeitig Fairness, Wettbewerb und Datenhoheit gewahrt bleiben.

Status: Inkrafttreten am 12. September 2025

Anwendbarkeit von Regeln zum Datenaustausch

Die EU-Datenverordnung tritt am 12. September 2025 in Kraft. Sie gilt in der gesamten Europäischen Union und legt Rechte und Pflichten für Unternehmen und öffentliche Einrichtungen in Bezug auf den Zugang, den Austausch und die Nutzung von nicht personenbezogenen Daten fest. Die Datenverordnung ist besonders relevant für Unternehmen, die Cloud-Dienste, Produkte des Internets der Dinge (Internet of Things, IoT) und andere datenintensive Technologien entwickeln.

Wie die EU-DSGVO und die EU-KI-Verordnung wird auch die EU-Datenverordnung über die Grenzen der EU hinausgehen und für Nicht-EU-Unternehmen gelten, die in der EU tätig sind oder Produkte und/oder Dienstleistungen für Kunden mit Sitz in der EU anbieten. Diese extraterritoriale Anwendung stellt sicher, dass alle Organisationen, die Daten aus der EU verarbeiten, dieselben Regeln einhalten.

Wie die EU-DSGVO und die EU-KI-Verordnung müssen auch Schweizer Unternehmen, die datengesteuerte Produkte oder Dienstleistungen auf dem EU-Markt anbieten oder Daten mit EU-Unternehmen austauschen, die Einhaltung der EU-Datenverordnung sicherstellen. Dadurch wird gewährleistet, dass Schweizer Unternehmen wettbewerbsfähig bleiben und die Vorschriften vollständig einhalten, wenn sie in der digitalen Wirtschaft der EU tätig sind.

Compliance

Um die EU-Datenverordnung einzuhalten, müssen Unternehmen:

- Sicherstellen, dass sie über klare Prozesse für den Austausch nicht personenbezogener Daten verfügen, insbesondere in Bezug auf die Datenübertragbarkeit, Zugriffsrechte und Bedingungen für den Wechsel zu einem anderen Cloud-Dienst.
- Solide Vereinbarungen zum Datenaustausch entwickeln, die mit den in der Datenverordnung festgelegten Grundsätzen übereinstimmen und einen fairen Datenzugang für Dritte gewährleisten.
- Transparenz in Bezug auf die Bedingungen für den Datenzugriff schaffen und sicherstellen, dass die Nutzer, ob Unternehmen oder Verbraucher, die Kontrolle über die durch ihre Produkte oder Dienstleistungen generierten Daten haben.

Die EU-Datenverordnung schränkt auch die Möglichkeiten von Cloud-Anbietern hinsichtlich der Datenübertragbarkeit ein und verpflichtet sie, einen reibungslosen Übergang zwischen Dienstanbietern zu ermöglichen und eine Datensperre zu verhindern.

Wer ist betroffen?

Die EU-Datenverordnung wird eine Vielzahl von Branchen betreffen, insbesondere solche in datenzentrierten Sektoren wie IoT, Cloud Computing und KI. Unternehmen, die nicht personenbezogene Daten sammeln, verarbeiten und speichern, unterliegen den neuen Vorschriften, ebenso wie Einrichtungen des öffentlichen Sektors, die aus regulatorischen oder gesellschaftlichen Gründen auf Daten zugreifen.

Jedes Unternehmen, das Dienstleistungen oder Produkte innerhalb der EU anbietet oder Daten verarbeitet, die von EU-ansässigen Nutzern generiert wurden, muss die Datenverordnung einhalten. Diese Anforderung gilt auch für Nicht-EU-Unternehmen (einschliesslich Schweizer Unternehmen), die datengesteuerte Produkte oder Dienstleistungen auf dem EU-Markt anbieten oder Daten mit EU-Unternehmen austauschen.

Was ist zu tun?

Um auf die EU-Datenverordnung vorbereitet zu sein, empfehlen wir folgende Schritte:

- Überprüfen Sie Ihre aktuellen Datenaustauschpraktiken und stellen Sie sicher, dass sie den neuen Anforderungen an Transparenz und Fairness entsprechen.
- Führen Sie Prozesse für die Datenübertragbarkeit und den nahtlosen Wechsel zwischen Cloud-Anbietern ein, um die Einhaltung der Datenverordnung zu gewährleisten.
- Aktualisieren Sie Verträge und Service-Level-Vereinbarungen mit Dritten, um die Verpflichtungen in Bezug auf Datenzugriff und -nutzung zu berücksichtigen.

Ihr PwC-Team für Datenschutz und Compliance steht Ihnen zur Verfügung, um Ihre aktuellen Strategien für den Datenaustausch zu bewerten und sicherzustellen, dass Ihre Organisation bereit ist, die Herausforderungen und Chancen, die durch die EU-Datenverordnung entstehen, zu meistern.

2 International Standards on Auditing (ISA)

2.1 ISA 600 (Revised) „Besondere Überlegungen zu Konzernabschlussprüfungen (einschliesslich der Tätigkeit von Teilbereichsprüfern)“

Der Standard stärkt und erweitert die Verantwortung des Group Engagement Leaders für das Management und das Erreichen der Prüfungsqualität im Rahmen der Prüfung eines Konzernabschlusses sowie die Verantwortung des Konzernprüfers für die Gesamtleitung und Überwachung der Konzernabschlussprüfung und die Überprüfung der Arbeit der Teilbereichsprüfer.

Status:	Anzuwenden ist der Standard für Abschlussprüfungen von Geschäftsjahren, die am oder nach dem 15. Dezember 2023 beginnen

Zu den wesentlichen Änderungen am Standard gehören:

- Die Verantwortung des Konzernprüfers für die Konzernprüfung zusammen mit einer Änderung der Definition des Prüfungsteams.
- Grösserer Fokus auf den risikobasierten „Top-down“-Ansatz mit umfassenderen und spezifischeren Verantwortlichkeiten des Konzernprüfers für die Risikobeurteilung und die Planung eines risikoorientierten Prüfungsansatzes
- Überarbeitete Anforderungen und Erläuterungen für das Scoping von Konzernprüfungen zur Erleichterung eines risikoorientierten Ansatzes, der mehr Flexibilität bei der Entwicklung eines Konzernprüfungsplans erlaubt, um ausreichende geeignete Prüfungsnachweise zu erlangen (wo, was und von wem geprüft wird).
- Streichung des Konzepts der „bedeutsamen Teilbereiche“ und der damit verbundenen Anforderung, diese zu identifizieren und einen „Full scope audit“ (Prüfung) der bedeutsamen Teilbereiche durchzuführen, welche für sich genommen von wirtschaftlicher Bedeutung für den Konzern sind.
- Streichung der „Review der Finanzinformationen eines Teilbereichs“ als eine Art von Tätigkeit, welche in Bezug auf Finanzinformationen eines Teilbereichs durchgeführt werden können.