



KI-Compliance zwischen Innovation, Regulierung und digitaler Souveränität

Prüfbare Governance nach dem AI Act für Revision, Datenschutz und IT-Sicherheit

(Stand 15. Juni 2026)

Zusammenfassung

Künstliche Intelligenz ist für Unternehmen und öffentliche Stellen nicht mehr nur ein Innovationsprojekt der Fachabteilungen. Sie wird zu einem Gegenstand der Revision, der Datenschutzorganisation, der Informationssicherheit und des Einkaufs. Der AI Act zwingt Organisationen dazu, KI nicht allein technisch, sondern als beherrschbaren Prozess zu verstehen: mit Risikoklassifizierung, Rollenklärung, dokumentierten Freigaben, menschlicher Aufsicht, Monitoring und belastbaren Nachweisen. Gerade für Revisorinnen und Revisoren ist die zentrale Frage daher nicht, ob KI eingesetzt wird, sondern ob die Organisation weiß, wo, wofür, durch wen und mit welchen Kontrollmechanismen KI eingesetzt wird.

Der Beitrag skizziert einen praxisnahen Prüfungsrahmen. Er verbindet die risikobasierte Logik des AI Act mit den Anforderungen der DSGVO, der IT-Sicherheit und einer zunehmend wichtigen Dimension digitaler Souveränität. Compliance soll Innovation nicht blockieren. Sie soll Entscheidungsfähigkeit herstellen: Eine Organisation, die ihre KI-Systeme inventarisiert, klassifiziert und kontrolliert, kann schneller und rechtssicherer innovieren als eine Organisation, die auf Schatten-KI und nachträgliche Krisenbewältigung setzt.

1. Ausgangspunkt: KI ist kein isoliertes Technikthema

Viele KI-Projekte beginnen harmlos: ein Sprachmodell für Textentwürfe, ein Analysewerkzeug für Kundenanfragen, eine Software zur Priorisierung von Tickets, ein System zur Betrugserkennung oder ein Tool zur Vorauswahl von Bewerbungen. Rechtlich relevant wird KI jedoch nicht erst, wenn ein Schaden eintritt oder eine Behörde nachfragt. Risiken entstehen bereits bei Zweckbestimmung, Datenbasis, Rollenverteilung, Beschaffung, Integration und Betrieb. Die technische Attraktivität eines Systems sagt wenig darüber aus, ob sein Einsatz rechtlich zulässig, prüfbar und organisatorisch beherrschbar ist.

Für die Praxis ist deshalb ein Perspektivwechsel erforderlich. KI-Compliance ist nicht die nachträgliche Erstellung eines Dokuments, das ein bereits laufendes System legitimieren soll. Sie ist eine vorgelagerte und fortlaufende Steuerung. Der rechtliche Maßstab folgt nicht dem Marketingetikett des Produkts, sondern dem konkreten Einsatzkontext. Ein identisches Modell kann als einfache Textassistentz geringes Risiko haben, im Bewerberranking dagegen in die Nähe eines Hochrisiko-Systems rücken. Ebenso kann eine scheinbar unterstützende Prognose faktisch entscheidungsprägend werden, wenn Menschen die Ergebnisse nur noch abnicken.

Damit wird KI auch zu einem klassischen Revisi-onsthema. Die Revision fragt nach Angemessenheit und Wirksamkeit des internen Kontrollsystems. Bei KI heißt das: Gibt es ein vollständiges Inventar? Gibt es einen Freigabeprozess? Sind Verantwortlichkeiten klar benannt? Werden Datenflüsse, Eingabedaten, Modell-änderungen, Logs und Vorfälle erfasst? Kann die Orga-nisation im Streitfall erklären, warum ein System zu-lässig war und wie es überwacht wurde? Ohne solche Nachweise bleibt KI-Compliance im Kern eine Behaup-tung.

2. Der AI Act als risikobasierter Ordnungsrahmen

Die Verordnung (EU) 2024/1689 folgt einem risikoba-sierten Ansatz. Sie unterscheidet insbesondere verbote-ne Praktiken, Hochrisiko-Systeme, transparenzpflich-tige Anwendungen und Systeme mit minimalem oder geringem Risiko. Hinzu kommen Regeln für General-Purpose-AI-Modelle (GPAI), also Modelle mit breitem Einsatzspektrum. Die einzelnen Pflichtenkreise greifen zeitlich gestaffelt. Seit dem 2. Februar 2025 gelten insbe-sondere die Verbote bestimmter KI-Praktiken sowie die Pflicht zur KI-Kompetenz. Seit dem 2. August 2025 sind

Pflichten für Anbieter von GPAI-Modellen anwendbar. Transparenzpflichten, etwa bei bestimmten Formen der Interaktion mit KI oder bei synthetischen Inhalten, gewinnen spätestens ab August 2026 operative Bedeu-tung. Für Hochrisiko-Systeme sind nach der politischen Einigung zum AI-Omnibus verlängerte Übergangsfris-ten vorgesehen, insbesondere für Annex-III-Anwendun-gen bis 2. Dezember 2027 und für produktintegrierte Hochrisiko-KI bis 2. August 2028.

Aus Compliance-Sicht ist entscheidend, dass diese Zeitachse nicht als Aufschub missverstanden wird. Or-ganisationen benötigen schon jetzt ein Verfahren, um Use Cases zu identifizieren, Rollen zu bestimmen und Verbotsrisiken auszuschließen. Die wichtigste Sofort-maßnahme ist kein umfassendes Rechtsgutachten zu jedem denkbaren Einzelfall, sondern ein funktionieren-der Eingangstest. Er beginnt mit drei Fragen: Handelt es sich überhaupt um ein KI-System im Sinne des AI Act? Welche Rolle nimmt die Organisation ein? In welchem Risikosegment liegt der konkrete Einsatz?

Die erste Frage ist nicht trivial. Klassische Software ist nicht automatisch KI; zugleich kann KI in scheinbar einfachen Workflows verborgen sein. Maßgeblich ist, ob ein System aus Eingaben Ergebnisse wie Vorhersa-gen, Inhalte, Empfehlungen oder Entscheidungen ablei-tet und dabei ein gewisser Grad an Autonomie besteht. Grenzfälle sollten dokumentiert werden, weil alle weite-ren Prüfungen auf dieser Grundannahme aufbauen.

3. Von der Risikoklasse zur Prüfspur

Die Risikoklassifizierung darf nicht an die IT-Abteilung delegiert werden, ohne den Fachkontext einzubezie-hen. Technik beschreibt, was ein System kann. Recht-lich relevant ist, wofür es eingesetzt wird und welche Wirkungen es erzeugt. Ein Sprachmodell, das interne Formulierungsvorschläge liefert, ist anders zu bewerten als ein Modell, das Bürgeranträge priorisiert, Kreditrisi-ken bewertet oder Bewerbungen sortiert. Die Risikoklas-se entsteht aus System, Zweck, Kontext und Folgen.

Verbotene Praktiken bilden die rote Linie. Dazu ge-hören insbesondere manipulative oder ausnutzende An-wendungen, bestimmte Formen sozialen Scorings, un-zulässige biometrische Kategorisierung und bestimmte Emotionserkennungskontexte. Für die Organisation be-deutet das: Jeder KI-Pilot benötigt einen Verbotscheck. Dieser Check sollte in Beschaffung, Projektantrag und Freigabeformular sichtbar verankert sein. Eine verbote-ne Anwendung wird nicht dadurch rechtmäßig, dass sie gut dokumentiert oder technisch leistungsfähig ist.

Bei Hochrisiko-Systemen wird das Pflichten-programm erheblich dichter. Der AI Act kennt zwei

zentrale Eintrittstore. Annex I betrifft KI als Sicherheitskomponente oder Produkt in harmonisierten Produktregelungen. Annex III nennt Anwendungsfelder wie Beschäftigung, Bildung, kritische Infrastruktur, Migration, Strafverfolgung, Justiz und demokratische Prozesse. Besonders praxisrelevant ist die Frage, ob eine Annex-III-Anwendung ausnahmsweise kein erhebliches Risiko begründet. Eine solche Ausnahme muss vor dem Einsatz begründet und dokumentiert werden. Sie sollte nicht routinemäßig angenommen werden, wenn Profiling, entscheidungsrelevante Bewertung oder vulnerable Gruppen betroffen sind.

Für die Revision ist die Risikoklasse kein abstraktes Etikett, sondern der Beginn einer Prüfspur. Zu jeder Einordnung gehören Datum, Verantwortliche, zugrunde gelegter Zweck, Datenbasis, betroffene Personen, Ergebnis der Verbotsprüfung, Rolle der Organisation und geplante Kontrollen. Ändert sich der Zweck, die Datenklasse, das Modell, die Nutzergruppe oder der Anbieter, ist die Einstufung erneut zu prüfen. KI-Compliance ist daher lebenszyklusbezogen.

4. Rollen in der Lieferkette: Anbieter, Betreiber und der schleichende Rollenwechsel

Der AI Act arbeitet mit funktionalen Rollen. Anbieter ist, wer ein KI-System entwickelt oder entwickeln lässt und unter eigenem Namen in Verkehr bringt oder in Betrieb nimmt. Betreiber ist, wer ein KI-System in eigener Verantwortung beruflich nutzt. Hinzu kommen unter anderem Importeure und Händler. Die Praxis neigt dazu, diese Rollen vertraglich zu vereinfachen: Man kauft doch nur ein Tool ein, also sei der Anbieter verantwortlich. Diese Sicht ist gefährlich verkürzt.

Betreiberpflichten bleiben auch bei zugekauften Systemen relevant. Betreiber müssen Hochrisiko-Systeme nach Gebrauchsanweisung einsetzen, menschliche Aufsicht organisieren, Eingabedaten kontrollieren, Monitoring ermöglichen und gegebenenfalls betroffene Personen informieren. Noch wichtiger ist der mögliche Rollenwechsel. Wer ein System wesentlich verändert, unter eigenem Namen bereitstellt oder eine neue Zweckbestimmung festlegt, kann in Anbieterpflichten hineinwachsen. Customization, Fine-Tuning, Integration in eigene Prozesse und erhebliche Zweckänderungen müssen deshalb rechtlich bewertet werden.

Hier liegt ein praktisches Revisionsrisiko. Fachbereiche experimentieren mit Modellen, IT integriert APIs, der Einkauf verhandelt Standardverträge, Datenschutz prüft Datenverarbeitungen und die Rechtsabteilung wird spät eingebunden. Das Ergebnis kann eine

Verantwortungsdiffusion sein, bei der niemand den Rollenwechsel erkennt. Ein KI-Kontrollsystem muss deshalb festlegen, welche Änderungen freigabepflichtig sind und ab wann ein erneuter Rollen- und Risikotest ausgelöst wird.

5. DSGVO und AI Act: integrierte Folgenabschätzung statt Doppelprüfung

KI-Compliance steht selten isoliert. Sobald personenbezogene Daten verarbeitet werden, bleiben die Anforderungen der DSGVO eigenständig relevant. Rechtsgrundlage, Zweckbindung, Datenminimierung, Speicherfristen, Transparenz, Betroffenenrechte, technische und organisatorische Maßnahmen sowie gegebenenfalls eine Datenschutz-Folgenabschätzung sind zu prüfen. Der AI Act erweitert diese Perspektive um Sicherheit, Grundrechte, Modellrisiken, Daten-Governance, Robustheit, menschliche Aufsicht und Nachweisführung.

In der Praxis sollten Organisationen deshalb keine parallelen Papierwelten schaffen. Sinnvoll ist ein integriertes KI-Assessment, das datenschutzrechtliche und KI-spezifische Risiken gemeinsam erfasst. Eine solche Prüfung sollte mindestens folgende Felder enthalten: Zweck und Entscheidungskontext, personenbezogene und nicht personenbezogene Daten, Datenherkunft, Rechtsgrundlage, Datenqualität, potenzielle Benachteiligungen, technische Leistungsgrenzen, menschliche Aufsicht, Erklärbarkeit, Logging, Sicherheitsmaßnahmen und Beschwerdewege.

Besondere Aufmerksamkeit verdient Art. 22 DSGVO. Eine formal menschliche Beteiligung genügt nicht, wenn die Entscheidung faktisch durch das System determiniert wird. In vielen Organisationen entsteht Automatisierung nicht durch einen ausdrücklichen Vollautomaten, sondern durch Gewöhnung: Das System liefert Scores, Prioritäten oder Empfehlungen; die menschliche Stelle folgt ihnen regelmäßig, ohne echte Prüfung. Für die Revision ist daher nicht nur die Prozessbeschreibung entscheidend, sondern die gelebte Praxis. Werden Entscheidungen tatsächlich überprüft? Haben Aufsichtspersonen Zeit, Kompetenz und Befugnis zum Override? Gibt es Eskalationswege bei auffälligen Outputs?

6. Governance: Mindestarchitektur für prüfbare KI

Eine wirksame KI-Governance muss nicht mit einem Großprojekt beginnen. Sie benötigt aber einige unver-

zichtbare Bausteine. Erstens ein KI-Inventar. Erfasst werden sollten Use Case, Zweck, System, Anbieter, Modelltyp, Datenquellen, Nutzergruppen, betroffene Personen, Rolle der Organisation, Risikoklasse, Betriebsstatus, Owner, Freigabedatum und Review-Termin. Das Inventar muss auch Piloten, Testsysteme und Fachbereichstools einschließen. Gerade dort entsteht Schatten-KI.

Zweitens braucht es einen risikosensiblen Freigabeprozess. Niedrigschwellige Anwendungen sollten schnell und standardisiert geprüft werden können; Hochrisiko- und Grenzfälle benötigen eine vertiefte Bewertung und gegebenenfalls Managemententscheidung. Beteiligte Funktionen sind typischerweise Fachbereich, IT, Datenschutz, Informationssicherheit, Recht, Einkauf und Revision. Die Freigabe sollte nicht nur Ja oder Nein lauten, sondern Bedingungen enthalten: zulässige Daten, Nutzerkreis, Aufsichtsregeln, Dokumentationspflichten, Monitoringparameter und Review-Termin.

Drittens ist KI-Kompetenz zu organisieren. Die Pflicht zur AI Literacy verlangt keine abstrakte Bildungsoffensive, sondern rollenbezogene Befähigung. Einkauf muss Due-Diligence-Fragen stellen können. Fachbereiche müssen erlaubte und verbotene Nutzung verstehen. Datenschutz und Informationssicherheit müssen Datenflüsse, Prompt-Risiken und Logging bewerten können. Management muss Risiken priorisieren und Ressourcen bereitstellen. Schulungen sollten daher nicht nur technische Begeisterung vermitteln, sondern Grenzen, Halluzinationen, Geheimnisschutz, Urheberfragen, Output-Kontrolle und Eskalationsregeln behandeln.

Viertens muss die Dokumentation auffindbar, versioniert und verständlich sein. Relevant sind Systemsteckbrief, Risikomatrix, Datenbeschreibung, Testnachweise, Nutzungsanweisung, Freigabeentscheidung, Vertragsunterlagen, Monitoringprotokolle und Änderungsdocumentation. Dokumentation ist nicht Papierproduktion. Sie ist Beweisführung. Was nicht auffindbar, aktuell und verständlich ist, existiert im Prüfungsfall praktisch nicht.

7. Beschaffung als Compliance-Hebel

Viele KI-Risiken werden im Einkauf entschieden. Wenn Vertrag und technische Architektur keinen Zugriff auf erforderliche Informationen, keine Logs, keine Auditunterstützung, keine Änderungsmitteilungen und keinen Exit ermöglichen, kann die Organisation ihre eigenen Pflichten später kaum erfüllen. Deshalb muss KI-Beschaffung frühzeitig mit Compliance verbunden werden.

Vor Vertragsschluss sind mindestens Risikoklasse, Rolle, Zweck, Datenflüsse, Sicherheitsniveau, Subunternehmer, Drittlandbezüge, Modelländerungen, Supportpflichten und Löschkonzept zu klären. Bei GPAI- und Cloud-KI sind Modellkarten, Nutzungsbeschränkungen, Trainingsdatenzusammenfassungen, Sicherheitsmaßnahmen, systemische Risiken und vertragliche Beschränkungen relevant. Der Anbieter muss Informationen liefern, die interne Prüfung, Betroffenenkommunikation und Behördenanfragen ermöglichen.

Kernklauseln betreffen technische Dokumentation, Auditunterstützung, Zugriff auf relevante Logs, Mitteilung wesentlicher Änderungen, Incident-Kommunikation, Unterstützung bei Behörden- und Betroffenenanfragen, Löschung, Portabilität und Exit. Pilotverträge verdienen besondere Aufmerksamkeit. Sobald reale Daten oder reale Entscheidungen betroffen sind, ist ein Pilot kein folgenloses Experiment mehr. Die spätere Compliance-Fähigkeit entscheidet sich dann bereits im Teststadium.

8. Monitoring nach Go-live: der Betrieb als Risikophase

Der Go-live beendet die KI-Prüfung nicht. Häufig entstehen Risiken gerade im Betrieb: Daten ändern sich, Nutzergruppen erweitern sich, Modelle werden aktualisiert, Prompts werden kreativer, Workflows verschieben sich, Fehlerraten steigen oder Beschwerden nehmen zu. Hinzu kommen Model Drift, Security-Angriffe und unerwartete Zweckänderungen. Ein System, das bei Freigabe vertretbar war, kann später anders zu bewerten sein.

Monitoring benötigt daher messbare Parameter. Dazu gehören Fehlerraten, Auffälligkeiten, Beschwerden, Override-Quoten, Drift-Indikatoren, Systemausfälle, Sicherheitsereignisse und Änderungen an Modell oder Datenbasis. Wichtig sind Schwellenwerte und Reaktionspläne. Wer erkennt ein Problem? Wer entscheidet über Abschaltung, Einschränkung oder Nachschulung? Wann wird die Rechts- oder Datenschutzprüfung erneut ausgelöst? Wie werden Vorfälle dokumentiert?

Für die Revision ist Monitoring ein Wirksamkeitsnachweis. Eine Policy zeigt nur die Soll-Ordnung. Monitoring zeigt, ob sie im Betrieb funktioniert. Besonders wertvoll sind Managementberichte, die nicht nur Aktivität abbilden, sondern Risiko: Anzahl der Use Cases, Verteilung nach Risikoklassen, offene Freigaben, kritische Abhängigkeiten, nicht abgeschlossene Reviews, Vorfälle, Maßnahmen und Rest-Risiken. So wird KI-Compliance entscheidungsfähig.

9. Digitale Souveränität als neue Compliance-Dimension

Neben Zulässigkeit, Datenschutz und Sicherheit tritt eine weitere Frage: Bleibt der KI-Einsatz beherrschbar? Digitale Souveränität meint dabei keine Autarkie und kein pauschales Misstrauen gegenüber bestimmten Herkunftsländern. Gemeint ist die Fähigkeit, Abhängigkeiten zu erkennen, zu begrenzen und im Ernstfall handlungsfähig zu bleiben. Für KI ist diese Frage besonders relevant, weil Kontrolle über Daten, Modelle, Schlüssel, Logs, APIs, Rechenkapazitäten und Updatepfade verteilt ist.

Die jüngere europäische Tech-Sovereignty-Debatte und der Vorschlag eines Cloud and AI Development Act zeigen, dass Infrastrukturfragen unmittelbare Compliance-Relevanz haben. Speicherort allein genügt nicht. Bei Cloud- und KI-Diensten sind Konzernkontrolle, Administrationszugriffe, Subprozessoren, Schlüsselverwaltung, Datenexport, Modellportabilität und rechtliche Zugriffspfade zu berücksichtigen. Für sensible Prompts, HR-Daten, Forschungsdaten, Mandatsinformationen oder vertrauliche Unternehmensdaten steigen die Anforderungen an Segmentierung, Pseudonymisierung, Verschlüsselung, Schlüsselhoheit und Datenminimierung.

Praktisch sollte das KI-Inventar deshalb um eine Souveränitätsspalte ergänzt werden. Erfasst werden können Modellanbieter, Hosting-Ort, Konzernkontrolle, Subprozessoren, Administrationszugriffe, Exportmöglichkeiten, Exit-Aufwand, Schlüsselkontrolle und Kritikalität des Prozesses. Die Bewertung sollte zwischen bloßer Komfortabhängigkeit, wirtschaftlichem Lock-in und nicht beherrschbarer Kritikalität unterscheiden. Ein Textassistententool für allgemeine Formulierungen ist anders zu behandeln als eine proprietäre KI-Infrastruktur, auf der zentrale Verwaltungs- oder Finanzprozesse beruhen.

Vergaberechtlich und vertraglich führt dies nicht zwingend zu einem pauschalen Herkunftsausschluss. Tragfähiger sind objektive funktionale Anforderungen: Zugriffskontrolle, Schlüsselhoheit, Portabilität, Auditierbarkeit, Exit-Test, Verfügbarkeit, Sicherheitszertifizierungen, transparente Subunternehmerstruktur und Unterstützung bei Drittstaatenzugriffen. Open Source, EU-basierte Modelle, private Instanzen und On-Prem-Optionen können Prüfbarkeit und Verhandlungsmacht verbessern, ersetzen aber keine Sicherheits- und Qualitätsprüfung. Souveränität ist graduell. Schon partielle Ausweichfähigkeit stärkt Resilienz.

10. Praxisbeispiele für die Prüfung

Personal-KI ist ein besonders sensibler Anwendungsfall. Systeme zur Vorauswahl, zum Ranking oder zur Leistungsbewertung können Zugangschancen erheblich beeinflussen. Prüfungsfragen betreffen Datenrepräsentativität, Bias, Transparenz gegenüber Bewerberinnen und Bewerbern, Beteiligung der Arbeitnehmervertretung und echte menschliche Entscheidungsmacht. Der Begriff Assistenztool sollte hier nicht beruhigen. Entscheidend ist, ob die Empfehlung faktisch die Entscheidung prägt.

Bei generativer KI im Büro liegen die Risiken anders. Häufig geht es nicht um Hochrisiko-KI, sondern um Geheimnisschutz, Halluzinationen, Urheberfragen, falsche Außenkommunikation und unkontrollierte Datenweitergabe. Eine gute Policy unterscheidet erlaubte Daten, verbotene Eingaben, Freigabeerfordernisse, Kennzeichnungspflichten und Qualitätskontrollen. Externe Kommunikation darf nicht allein auf KI-Output beruhen, wenn fachliche Verantwortung, Reputation oder rechtliche Bindung betroffen sind.

Im Finanzbereich stehen Scoring, Betrugserkennung und Risikoprognosen im Mittelpunkt. Hier verbinden sich AI Act, DSGVO, Verbraucherschutz, IT-Sicherheit und Revisionsanforderungen. Relevante Fragen sind Schwellenwerte, Fehlalarmkontrolle, Beschwerdewege, Erklärbarkeit, Datenqualität und Auditierbarkeit. Je stärker ein Ergebnis Zugang zu Leistungen, Verträgen oder Konditionen beeinflusst, desto höher sind die Anforderungen an Fairness, Nachvollziehbarkeit und menschliche Kontrolle.

In der öffentlichen Verwaltung kommt die Verfahrensdimension hinzu. KI darf Verfahren unterstützen, aber nicht die rechtliche Verantwortung verdrängen. Priorisierung, Risikohinweise oder Textvorschläge können nützlich sein. Sobald sie die Entscheidung über Leistungen, Pflichten oder Rechtsschutzchancen prägen, steigen die Anforderungen an Begründung, Gleichbehandlung, Anhörung und Überprüfbarkeit.

11. Revisionsorientierte Prüffragen

Für eine Erstprüfung können folgende Fragen als Mindeststandard dienen:

Prüffrage	Revisionsrelevanz
Gibt es ein vollständiges KI-Inventar einschließlich Piloten und Fachbereichstools?	Ohne Inventar sind Risikoklassifizierung, Verantwortlichkeit und Monitoring nicht prüfbar.
Sind für jeden Use Case Zweck, Rolle und Risikoklasse dokumentiert?	Die rechtliche Bewertung hängt vom konkreten Einsatzkontext und nicht vom Produktnamen ab.

Wurde ein Verbotscheck durchgeführt?	Verbotene Praktiken sind nicht durch Dokumentation oder Einwilligung heilbar.
Sind Datenflüsse, Rechtsgrundlagen und DSFA-Bedarf geprüft?	AI Act und DSGVO müssen in einem konsistenten Assessment zusammengeführt werden.
Gibt es wirksame menschliche Aufsicht?	Aufsicht erfordert Kompetenz, Zeit, Befugnisse und dokumentierte Override-Möglichkeiten.
Sichern Verträge Dokumentation, Logs, Audit, Änderungsmitteilungen und Exit?	Beschaffung entscheidet über spätere Nachweis- und Durchsetzungsfähigkeit.
Werden Drift, Fehlerraten, Beschwerden und Vorfälle überwacht?	Go-live ist der Beginn der Betriebsprüfung, nicht ihr Ende.
Sind kritische Abhängigkeiten und Souveränitätsrisiken sichtbar?	Lock-in, Drittstaatenzugriffe und fehlende Portabilität können Compliance praktisch entwerfen.

12. Ein realistischer 90-Tage-Plan

Viele Organisationen zögern, weil die Detailfragen des AI Act komplex sind und Standards, Leitlinien und nationale Zuständigkeiten fortlaufend konkretisiert werden. Dieses Zögern ist verständlich, aber riskant. Ein praktikabler Einstieg kann in 90 Tagen erfolgen.

In den ersten 30 Tagen sollten Verantwortliche benannt, ein einfaches KI-Inventar aufgebaut, bekannte Use Cases gesammelt und ein Verbotscheck eingeführt werden. Parallel sollte eine Kurz-Policy definieren, welche Nutzungen erlaubt, eingeschränkt oder untersagt sind. In den Tagen 31 bis 60 folgen ein Klassifizierungsschema, ein integriertes Datenschutz- und KI-Assessment, erste Beschaffungsfragen und Musterklauseln. In den Tagen 61 bis 90 sollten Pilotfreigaben, Schulungen, Monitoringkonzept und ein Managementreport umgesetzt werden.

Dieser Plan löst nicht jede Spezialfrage. Er schafft aber Steuerungsfähigkeit. Die Organisation weiß danach, wo KI eingesetzt wird, wer verantwortlich ist, welche Risiken prioritär sind und welche Nachweise fehlen. Genau diese Transparenz ist die Grundlage für weitere Vertiefung.

13. Fazit

Innovationsfreundliche KI-Compliance ist strukturiertes Risikomanagement. Sie beginnt mit Klassifizierung, Rollenprüfung und Verbotscheck; sie wird durch Governance, Dokumentation, Beschaffung, Monitoring und Schulung operationalisiert; sie bleibt wirksam, wenn Abhängigkeiten und Souveränitätsrisiken sichtbar werden. Für Revision, Datenschutz und IT-Sicherheit entsteht damit ein gemeinsames Arbeitsfeld.

Die zentrale Botschaft lautet: KI darf nicht unsichtbar bleiben. Eine Organisation muss erklären können, welche KI sie einsetzt, wofür sie sie einsetzt, auf welcher Datenbasis sie arbeitet, wer Aufsicht führt, welche Kontrollen bestehen und wie Fehler erkannt werden. Nicht regulatorische Perfektion ist der erste Schritt, sondern nachweisbare Beherrschbarkeit. Wer diese Strukturen früh aufbaut, gewinnt nicht nur Rechtssicherheit, sondern auch Innovationsgeschwindigkeit.

Quellen und Bezugspunkte

Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.

Europäische Kommission, AI Act, Umsetzung und Anwendungstermine, insbesondere Angaben zu Verbotsregeln, AI Literacy, GPAI, Transparenzpflichten und Hochrisiko-Systemen.

Europäische Kommission, Guidelines for providers of general-purpose AI models, Stand 28. April 2026.

Europäische Kommission, European Technological Sovereignty Package und Vorschlag für einen Cloud and AI Development Act, 3. Juni 2026.

Vortraggrundlage: Thomas Hoeren, KI-Compliance zwischen Innovation und Regulierung, 13. Hamburger Datenschutztage, Stand 8. Juni 2026.



Professor Dr. Thomas Hoeren ist Leiter des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) der Universität Münster und Adjunct Professor am Fraunhofer Institut für Angewandte Informationstechnik (FIT).

Nach dem Studium der katholischen Theologie und der Rechtswissenschaften in Münster, Tübingen und London arbeitete er als Professor für Internationales Wirtschaftsrecht an der Universität Düsseldorf. Er war 15 Jahre lang Richter am Oberlandesgericht Düsseldorf mit Schwerpunkt Urheberrecht und Patentrecht. Neben seiner Tätigkeit an der Universität Münster berät er Start-up-Unternehmen beim Schutz und bei der Verwertung ihres Know-hows mit rechtlichen Mitteln.

Weitere Infos finden sich unter <https://www.itm.nrw/>