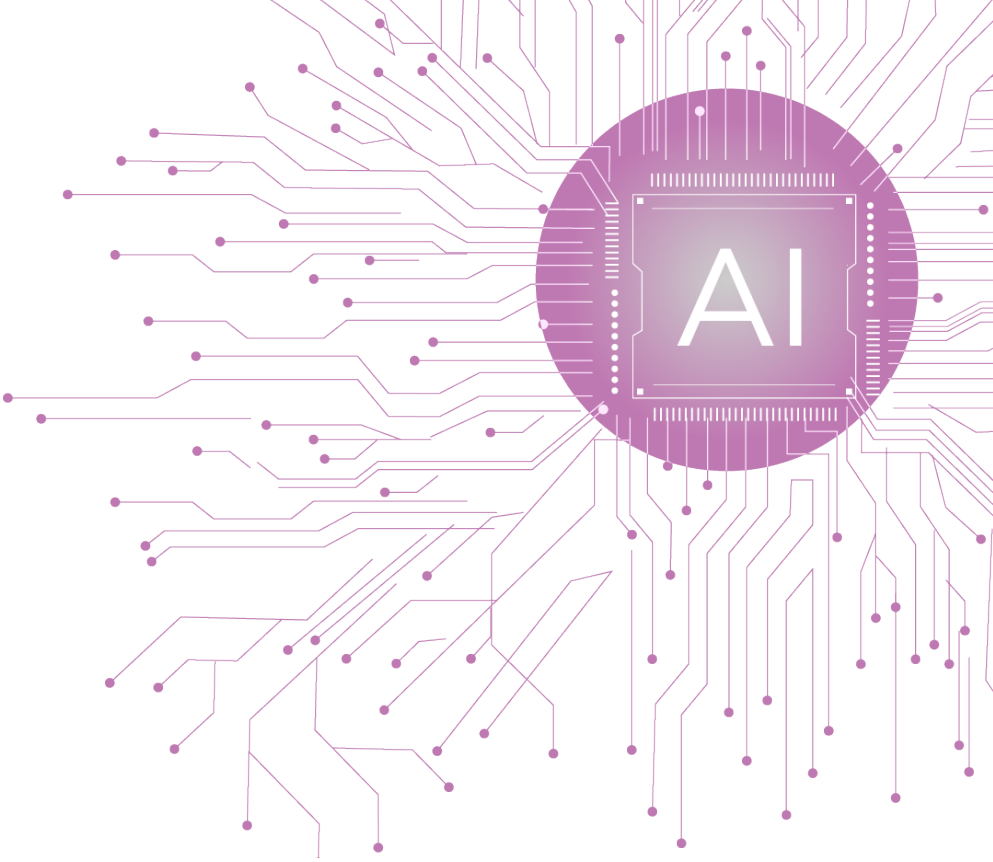
CLARIUS.LEGAL

Die EU-KI-Verordnung

Ein CLARIUS.LEGAL-Guide

www.clarius.legal



I. Einleitung

Was ist der Hintergrund für die EU-Verordnung über Künstliche Intelligenz?

Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie des 21. Jahrhunderts. Dank exponentieller Fortschritte in Algorithmen, Datenverfügbarkeit und Rechenleistung können KI-Systeme komplexe Aufgaben übernehmen, von der Automatisierung industrieller Prozesse bis hin zur Entscheidungsunterstützung in Medizin und Finanzwesen. Diese wachsende Bedeutung bringt jedoch auch erhebliche regulatorische Herausforderungen mit sich.

Die Europäische Union (EU) reagierte darauf mit einer Verordnung über Künstliche Intelligenz (kurz: KI-VO oder „AI Act"), die erstmals einen einheitlichen Rechtsrahmen für KI-Anwendungen in den Mitgliedstaaten geschaffen hat. Ziel ist es, einerseits Innovationen zu fördern und andererseits potenzielle Risiken für die Gesellschaft zu minimieren.

Dieses Whitepaper bietet einen ausführlichen Überblick über die Hintergründe, Ziele und Kerninhalte der KI-VO sowie über Herausforderungen und Handlungsempfehlungen für Unternehmen.

II. Hintergrund und Ziele der KI-VO

Technologische Entwicklungen und politischer Kontext

Die zunehmende Digitalisierung führt zu einer wahren Datenexplosion, da immer größere Mengen an Informationen generiert werden, die für das Training von KI-Systemen unerlässlich sind. Gleichzeitig sind die Kosten für Hochleistungs-Computing erheblich gesunken, wodurch selbst komplexe Deep-Learning-Modelle erschwinglicher und somit für eine breitere Anwendung nutzbar werden. In diesem Zusammenhang entwickelt sich ein intensiver globaler Wettbewerb, insbesondere zwischen den USA und China, wo große KI-Forschungszentren und Unternehmen entstehen, die das Potenzial haben, den europäischen Markt zu dominieren.

Gleichzeitig rücken jedoch auch Fragen zum Schutz von Grundrechten in den Fokus, da KI-Anwendungen tief in die Privatsphäre eingreifen oder diskriminierende Entscheidungen treffen können. Um solchen Risiken entgegenzuwirken, sollen Regulierungsmaßnahmen einen verantwortungs-vollen und sicheren Umgang mit Künstlicher Intelligenz gewährleisten.

II. Hintergrund und Ziele der KI-VO

Zentrale Zielsetzungen

Um diesen Umgang mit Künstlicher Intelligenz sicherzustellen, beschreibt die KI-Verordnung einige zentrale Zielsetzungen:

Förderung von Innovation
Durch klare Regeln und Rechtssicherheit sollen Unternehmen ermutigt werden, in KI zu investieren.

Risikobasierte Regulierung
Statt pauschaler Beschränkungen sollen gezielte Auflagen für besonders gefährliche Anwendungen eingeführt werden.

Wahrung der Grundrechte und EU-Grundwerte
Insbesondere der Schutz der Menschenwürde, der Privatsphäre und die Vermeidung von Diskriminierung sind zentrale Anliegen.

Transparenz und Verantwortung
Durch Dokumentations- und Kennzeichnungspflichten soll nachvoll-ziehbar bleiben, wie KI-Systeme Entscheidungen treffen und wer dafür verantwortlich ist.

III. Entstehungsgeschichte und gesetzlicher Rahmen

Vorläufer: Weißbuch und Strategie der EU-Kommission

Die Diskussion um einen europäischen Rechtsrahmen für KI begann bereits vor 2021. Im Februar 2020 veröffentlichte die EU-Kommission ein Weißbuch zur Künstlichen Intelligenz, in dem ein risikobasierter Ansatz skizziert wurde. Dort wurden bereits die Bereiche identifiziert, in denen KI zu besonders hohen Risiken für Gesundheit, Sicherheit und Grundrechte führen kann.

III. Entstehungsgeschichte und gesetzlicher Rahmen

Gesetzgebungsverfahren: Europäische Kommission, Rat und Parlament

Im April 2021 legte die Europäische Kommission ihren ersten Vorschlag für den AI Act vor (COM(2021) 206 final). Nach einer Phase der Kommentierung und Änderungsvorschläge begannen die Trilog-Verhandlungen, in denen die Kommission, der Rat der EU und das Europäische Parlament über den finalen Gesetzestext verhandelten. Schließlich wurde die Verordnung im Dezember 2023 vom Europäischen Parlament und dem Rat verabschiedet.

III. Entstehungsgeschichte und gesetzlicher Rahmen

Bezüge zu anderen Rechtsakten

Die KI-Verordnung (KI-VO) steht nicht isoliert, sondern ergänzt und erweitert bestehende rechtliche Rahmenwerke in der EU.

Die **Datenschutz-Grundverordnung (DSGVO)** enthält bereits Bestimmungen zum Schutz personenbezogener Daten. Die KI-VO baut hierauf auf, indem sie spezifische Anforderungen an KI-Systeme formuliert, die personenbezogene Daten verarbeiten.

Die KI-VO verweist teilweise auf bestehende **Produktsicherheitsrichtlinien** erweitert diese jedoch für KI-spezifische Risiken. Ab dem 20.01.2027 gilt die neue Europäische Maschinenverordnung. Diese berücksichtigt auch neue Entwicklungen wie KI und Autonomie.

Am 09.12.2024 ist zudem die neue **Produkthaftungsrichtlinie** in Kraft getreten. Auch KI-basierte Produkte gelten seither als „Produkte“ im Sinne des Produkthaftungsrechts. Außerdem wurde die Haftung stark erweitert

IV. Anwendungsbereich und Grundprinzipien

Breite Definition von KI und risikobasierter Ansatz

Die Verordnung definiert KI sehr weit, um auch künftige Technologien zu erfassen. Als „KI-System“ gelten Maschinen oder Software, die zum Beispiel Machine Learning, Deep Learning, regelbasierte Systeme, statistische Verfahren und ähnliche Techniken nutzen, um aus Daten Erkenntnisse abzuleiten und eigenständig Entscheidungen oder Vorhersagen zu treffen.

Das Kernstück der KI-VO ist ihr risikobasierter Ansatz. Die Anwendungen werden gemäß ihrem Gefährdungspotenzial für Gesundheit, Sicherheit und Grundrechte eingeteilt. Je höher das Risiko, desto strenger die Auflagen.

V. Risikokategorien und Beispiele

Verbotene KI-Systeme (Unacceptable Risk)

Diese Kategorie umfasst KI-Anwendungen, die gegen fundamentale Werte und Rechte in der EU verstoßen. Beispiele sind:

- **Manipulative KI-Systeme**:
  KI, die bewusst menschliches Verhalten so manipuliert, dass Personen zu Handlungen veranlasst werden, die ihnen oder anderen erheblichen Schaden zufügen

- **Social Scoring**:
  Systeme, die Menschen systematisch in sozialen Kontexten bewerten oder einstufen (z. B. „Punktesysteme“), um Zugänge zu staatlichen oder privaten Dienstleistungen zu steuern

- **Echtzeit-Biometrische Überwachung im öffentlichen Raum**
  (in vielen Fällen, mit einigen eng definierten Ausnahmen, z. B. in akuten Terror- oder Fahndungssituationen)

V. Risikokategorien und Beispiele

Hochrisiko-KI-Systeme (High Risk)

Systeme, die in sicherheitskritischen oder grundrechtsrelevanten Bereichen eingesetzt werden. Beispiele sind:

- **Gesundheit und Medizin**:
  KI zur Diagnose, Therapiefindung oder Operationen (z. B. in Robotik-Systemen).

- **Kritische Infrastrukturen**:
  Steuerung im Transportwesen (autonomes Fahren), in der Energieversorgung oder Telekommunikation

- **Justiz und Verwaltung**:
  Entscheidungsfindung in Gerichtsverfahren, Visa-Entscheidungen, Asylverfahren, Polizeiarbeit

- **Beschäftigung, Personalmanagement und Bildung**:
  KI-Systeme für Bewerberauswahl, Mitarbeiterbewertung, Zuordnung zu Bildungsmaßnahmen

Für Hochrisiko-Systeme gelten strengere Anforderungen, u. a. in Bezug auf Dokumentation und Konformitätsbewertung, Risikomanagement, Datenqualität und Transparenzpflichten.

V. Risikokategorien und Beispiele

Geringeres Risiko und Transparenzpflichten

Zu dieser Kategorie gehören KI-Systeme, die zwar Risiken bergen können, aber nicht als hochrisikoreich eingestuft werden. Hauptsächlich werden hier Transparenzanforderungen gestellt, etwa Kennzeichnungspflichten, wenn KI direkt mit Endnutzerinnen und Endnutzern interagiert (z. B. Chatbots, digitale Assistenten, Deepfake-Technologien). Nutzerinnen und Nutzer müssen wissen, dass sie es mit einer KI-Anwendung zu tun haben und ggf. ob Inhalte synthetisch generiert sind.

V. Risikokategorien und Beispiele

Minimales Risiko

Systeme mit sehr geringem Risiko, z. B. KI in Videospielen, Spam-Filtern oder Bildbearbeitungsprogrammen, unterliegen kaum Vorgaben. Allerdings können branchen- oder technologiebezogene Verhaltenskodizes (Codes of Conduct) entwickelt werden, um Best Practices zu fördern.

VI. Zentrale Verpflichtungen und Anforderungen für Unternehmen

Risikomanagement und Governance

Unternehmen müssen ein Risikomanagementsystem einführen, das den gesamten Lebenszyklus eines KI-Systems abdeckt. In der Entwicklungs- und Designphase müssen potenzielle Risiken identifiziert werden, die beim Einsatz der KI auftreten können. Während der Test- und Validierungsphase gilt es sicherzustellen, dass das System zuverlässig funktioniert, sicher ist und die Grundrechte respektiert.

Auch im Echtbetrieb ist eine kontinuierliche Überwachung (Monitoring) erforderlich, um Fehlfunktionen, sicherheitsrelevante Vorfälle oder Diskriminierungen frühzeitig zu erkennen und zu beheben. Darüber hinaus sollte im Unternehmen eine klare Governance-Struktur etabliert werden, die Zuständigkeiten und Verantwortlichkeiten für den Einsatz von KI festlegt, beispielsweise durch die Ernennung eines KI-Compliance-Beauftragten.

VI. Zentrale Verpflichtungen und Anforderungen für Unternehmen

Datengovernance und Datenqualität

Das Ziel besteht darin, Verzerrungen (Bias) zu minimieren und eine faire sowie zuverlässige Funktionsweise von KI-Systemen sicherzustellen. Dafür sind mehrere Maßnahmen erforderlich. Hochwertige und repräsentative Datensätze spielen eine zentrale Rolle, da die Trainingsdaten ausreichend divers sein müssen, um diskriminierende Ergebnisse zu vermeiden.

Ebenso wichtig ist die Dokumentation der Datenquellen, um nachvollziehen zu können, woher die Daten stammen und in welchem Kontext sie erhoben wurden. Darüber hinaus muss die Datensicherheit gewährleistet sein, indem sensible Informationen durch Verschlüsselung, regelmäßige Sicherheitsupdates und Schutzmaßnahmen gegen unbefugten Zugriff abgesichert werden.

VI. Zentrale Verpflichtungen und Anforderungen für Unternehmen

Transparenz, Erklärbarkeit und Nutzungskennzeichnung

Hochrisiko-KI-Systeme sollten so gestaltet sein, dass ihre Ergebnisse zumindest in Grundzügen nachvollziehbar sind, um eine gewisse Erklärbarkeit (Explainability) zu gewährleisten. Zudem gelten Kennzeichnungspflichten, sodass Nutzer eindeutig erkennen können, wenn sie mit einer KI interagieren – beispielsweise in Chatbots, generierten Texten, Bildern oder Avataren. Darüber hinaus sollten Unternehmen bei komplexen KI-Anwendungen umfassende Benutzerinformationen bereitstellen, die über die Funktionsweise, Anwendungsgrenzen und mögliche Fehlerraten aufklären.

VI. Zentrale Verpflichtungen und Anforderungen für Unternehmen

Konformitätsbewertung und Zertifizierung

Hochrisiko-KI-Systeme unterliegen häufig einer vorherigen Konformitätsbewertung, bei der – ähnlich wie bei Medizinprodukten – geprüft wird, ob sie die gesetzlichen Anforderungen erfüllen. Je nach Art des KI-Systems kann dies durch eine Eigenbewertung (Self-Assessment) oder eine externe Zertifizierung erfolgen, bei der sogenannte „benannte Stellen" (Third-Party-Audits) die Prüfung übernehmen. Wird das System erfolgreich validiert, kann es eine CE-Kennzeichnung erhalten, die den Marktzugang in der EU erleichtert.

VI. Zentrale Verpflichtungen und Anforderungen für Unternehmen

Rollen: Anbieter, Nutzer, Importeure, Distributoren

Die Verordnung definiert verschiedene wirtschaftliche Akteure und ihre Pflichten:

- **Anbieter (Provider)**:
  Organisation, die das KI-System entwickelt oder in Verkehr bringt. Hauptverantwortung für Design, Entwicklung und Konformität.

- **Nutzer (User)**:
  Unternehmen oder Personen, die KI-Systeme in ihren Prozessen einsetzen (z. B. Arbeitgeber, die ein Recruiting-Tool nutzen). Sie müssen sicherstellen, dass sie die KI ordnungsgemäß anwenden und überwachen.

- **Importeure und Distributoren**:
  Wer KI-Systeme aus Drittländern einführt oder vertreibt, übernimmt ebenfalls Verantwortung, indem er die Einhaltung der EU-Vorschriften sicherstellt.

VII. Durchsetzung und Sanktionen

Ahndung von Verstößen gegen die KI-Verordnung

Die Mitgliedstaaten richten spezielle Marktüberwachungsbehörden ein, die die Einhaltung der KI-Verordnung (KI-VO) überprüfen. Ähnlich wie bei der DSGVO sind dabei empfindliche Geldbußen vorgesehen. Schwere Verstöße, wie die falsche Klassifizierung eines hochrisikoreichen Systems oder die systematische Verletzung von Transparenzpflichten, können Strafen in Höhe von mehreren Prozent des weltweiten Jahresumsatzes nach sich ziehen. Darüber hinaus können Abmahnungen, einstweilige Verfügungen und Unterlassungsanordnungen Unternehmen dazu verpflichten, den Einsatz bestimmter KI-Technologien einzustellen oder anzupassen.

VIII. Herausforderungen, Kritik und offene Fragen

Balance aus Innovation, Regulierung & Rechtsdurchsetzung

- **Technische und organisatorische Herausforderungen**
  Die Erklärbarkeit komplexer Algorithmen ist eine Herausforderung, da Methoden wie Deep Learning oft als „Black Boxes“ gelten. Die geforderte Nachvollziehbarkeit könnte Innovationen bremsen oder technische Grenzen aufzeigen. Zudem erschweren strenge Datenschutzvorgaben, etwa im Gesundheitswesen, den Zugang zu hochwertigen Trainingsdaten.

- **Innovation vs. Regulierung**
  Start-ups und KMU fürchten hohe Kosten und bürokratische Hürden durch Zertifizierungsprozesse. Zudem könnten strikte Vorschriften Europas Wettbewerbsfähigkeit gegenüber agileren Märkten wie den USA und China schwächen.

- **Rechtsdurchsetzung und grenzüberschreitender Markt**
  Die Durchsetzung der EU-Verordnung bei internationalen Anbietern bleibt herausfordernd. Gleichzeitig erfordert eine Harmonisierung einheitliche Kriterien und Kontrollen, um einen Regelungsflickenteppich zu vermeiden.

- **Dynamik der KI-Entwicklung**
  Der technologische Fortschritt erfordert eine flexible Verordnung, die neue KI-Technologien wie generative KI abdeckt. Gleichzeitig machen adaptive Systeme eine kontinuierliche Risikobewertung nötig, um regulatorische Anforderungen dauerhaft zu erfüllen.

IX. Handlungsempfehlungen für Unternehmen

Wichtige Maßnahmen für den sicheren KI-Einsatz

Risikoorientiertes Vorgehen
Bereits in der Planungsphase sollten Unternehmen potenzielle Risiken analysieren und gezielt mindern. Zudem ist es essenziell, die Kategorisierung des KI-Systems zu klären, insbesondere ob es als Hochrisiko-System eingestuft wird.

Aufbau von internen Strukturen und Prozessen
Ein strukturiertes KI-Compliance-Management umfasst die Festlegung von Verantwortlichkeiten (z. B. ein KI-Compliance-Officer) sowie standardisierte Prozesse für Dokumentation und Monitoring. Eine interdisziplinäre Zusammenarbeit zwischen Entwicklern, Datenschützern und Rechtsexperten stellt sicher, dass technische und regulatorische Anforderungen erfüllt werden.

Qualitäts- und Datenmanagement
Eine effektive Data Governance reduziert Bias und stellt den Datenschutz sicher. Klare Richtlinien zur Datenbeschaffung, -validierung und -pflege sowie regelmäßige Audits helfen, Fehler und Diskriminierung frühzeitig zu erkennen.

Transparenzstrategien
Die Nutzeraufklärung ist essenziell: Endnutzer und Kunden sollten über Funktion, Risiken und Grenzen der KI informiert werden. Zudem sollten Modelle gewählt werden, die je nach Anwendungsfall eine angemessene Erklärbarkeit ermöglichen.

Schulungen und Sensibilisierung
Mitarbeiterschulungen zu KI-Regulierung, Datenschutz und Ethik helfen, Anforderungen zu verstehen. Awareness-Programme fördern ein nachhaltiges Risikobewusstsein, insbesondere bei datengetriebenen Prozessen.

Zusammenarbeit mit Behörden und Zertifizierungsstellen
Bei hochrisikoreichen KI-Anwendungen kann eine frühzeitige Abstimmung mit Aufsichts- oder Zertifizierungsstellen helfen, regulatorische Anforderungen frühzeitig zu berücksichtigen. Der Austausch mit Netzwerken und Branchenverbänden erleichtert die Umsetzung und fördert den Wissenstransfer.

X. Ausblick und zukünftige Entwicklungen

Gesetzgebung, Haftung & internationale Zusammenarbeit

Die KI-Verordnung tritt gestaffelt in Kraft: Ab dem 2. Februar 2025 sind Maßnahmen zur KI-Kompetenz, etwa Schulungen, erforderlich. Die meisten übrigen Regelungen, insbesondere zu Risikobewertungen, gelten ab dem 2. August 2026. Weltweit gewinnt die KI-Regulierung an Bedeutung, und die EU-Verordnung könnte als Vorbild für andere Regionen dienen.

XI. Fazit

Der Druck auf Unternehmen steigt: Handeln Sie jetzt!

Die geplante KI-Verordnung der EU soll Innovation und Grundrechtsschutz vereinen. Ihr risikobasierter Ansatz reguliert Hochrisiko-Bereiche strenger als geringfügige Anwendungen. Unternehmen sollten frühzeitig Maßnahmen ergreifen. Dazu müssen sie u.a. bestehende und geplante KI-Anwendungen erfassen, Hochrisiko-KI identifizieren, KI-Kompetenzen prüfen, Schulungen durchführen und eine KI-Leitlinie erstellen.

Bei allem gilt:

- Risikomanagement und Governance sind das Fundament einer nachhaltigen KI-Strategie.
- Datengovernance und Transparenz sichern Rechtskonformität und Akzeptanz.
- Kooperation mit Behörden, Zertifizierungsstellen und Experten minimiert rechtliche Unsicherheiten.

Trotz möglicher Bürokratie kann die Verordnung auch Chancen eröffnen, indem sie europaweit Standards setzt und so das Vertrauen in KI-Anwendungen stärkt.

Erfahren Sie, wie CLARIUS.LEGAL Sie unterstützen kann.

Ihre Ansprechpartner

Dr. Arnt Glienke, LL.M., CCP
Rechtsanwalt, Leiter Compliance & Datenschutz
Certified Compliance Professional (CCP)

Matthias Schulz
Director Sales

+49 40 257 660 967
compliance@clarius.legal

Jetzt Kontakt aufnehmen!

anfrage@clarius.legal

CLARIUS.LEGAL

Über CLARIUS.LEGAL

Stetig wachsende, haftungsrelevante Regularien und interne Ansprüche wie Kostendruck, Fachkräftemangel und begrenzte interne Ressourcen – Unternehmen und Rechtsabteilungen sind mit zahlreichen Herausforderungen konfrontiert. Um diese optimal zu meistern und Risiken zu minimieren, benötigen sie Effizienz und Flexibilität bei gleichzeitiger Planungssicherheit. Und das in zahlreichen Rechtsgebieten.

Da das mit ausschließlich internen Ressourcen eine große Herausforderung darstellt, stehen wir Unternehmen mit genau diesen Ansätzen zur Seite. Immer mit einem Inhouse-Approach, maximaler Zeit- und Kosteneffizienz und höchsten Qualitätsansprüchen. Denn als Rechtsanwaltskanzlei der neuesten Generation können wir Sie mit Alternative Legal Service Providing, Legal Tech Solutions und Rechtsberatung genau so unterstützen, wie Sie uns benötigen.

2015 gegründet, unterstützen wir inzwischen über 180 Mandanten aller Unternehmensgrößen, national und international. Zu unseren Kunden zählen u.a. Bosch, GKN, Samsung, Vodafone, Stuttgart Netze und Ascorium. Unser Team aus inhouse-erfahrenen Rechtsanwälten, Volljuristen und Legal Experts unterstützt bedarfsentsprechend mit professioneller Qualitätskontrolle in allen wichtigen Rechtsgebieten und im Compliancebereich.

CLARIUS.LEGAL Rechtsanwaltsaktiengesellschaft
Rolandsbrücke 4, 20095 Hamburg
www.clarius.legal