ChatGPT

Businessplan zur Umsetzung der EU-KI-Verordnung

Zusammenfassung

Die europäische **KI-Verordnung (AI Act)** definiert erstmals ein umfassendes Regelwerk für **künstliche Intelligenz** in der EU [1]. Unternehmen aller Größen – vom Ein-Personen-Unternehmen bis zum Mittelstand – müssen sich darauf einstellen, **KI-Systeme risikobasiert** zu kontrollieren und entsprechend zu kennzeichnen. Dieser Businessplan bietet einen branchenunabhängigen Leitfaden, um die Anforderungen des AI Act umzusetzen. Zunächst wird das regulatorische Umfeld analysiert, einschließlich der **Risikoklassifizierung** von KI (von **unannehmbaren** über **hochriskante** bis **begrenzte** und **minimale Risiken**). Darauf aufbauend werden konkrete **Umsetzungsstrategien** beschrieben – von Transparenz- und Kennzeichnungspflichten über Datenschutz und Daten-Governance bis hin zu technischer Dokumentation, **Konformitätsbewertung** sowie Melde- und Überwachungspflichten. Besonderes Augenmerk gilt den **kreativen Berufen**, etwa bei der Nutzung generativer KI, um kreative Freiheiten mit regulatorischen Vorgaben in Einklang zu bringen. Abschließend werden **Risiken und Chancen** der KI-Verordnung für Unternehmen bewertet und **Handlungsempfehlungen** ausgesprochen. Ein Anhang mit **Checkliste, Tools und Links** erleichtert die praktische Umsetzung. Kurz gesagt: Dieser Plan soll Unternehmen Orientierung geben, um **rechtskonforme, verantwortungsvolle KI** einzusetzen und dabei von neuen Möglichkeiten zu profitieren.

Zielsetzung

Ziel dieses Businessplans ist es, Unternehmen eine **strategische Anleitung** zur Umsetzung der EU-KI-Verordnung zu bieten. Unabhängig von Branche und Unternehmensgröße sollen folgende Ziele erreicht werden:

- **Rechtskonformität sicherstellen:** Alle Vorgaben der KI-Verordnung – von der Einstufung der KI-Systeme bis zur Dokumentation – vollständig erfüllen, um Bußgelder oder Vertriebsverbote zu vermeiden (die Verordnung sieht Strafen von bis zu 35 Millionen Euro bzw. 7 % des weltweiten Jahresumsatzes vor) [1].
- **Branchenunabhängige Anwendbarkeit:** Der Plan gilt als Rahmen für **alle Branchen und Anwendungen** von KI – von industrieller Fertigung über Gesundheitswesen und Personalwesen bis zur Kunst- und Kreativwirtschaft. Jedes Unternehmen soll die Inhalte auf seine eigenen Produkte, Dienstleistungen und Prozesse übertragen können.
- **Risikominimierung & Vertrauensbildung:** Durch proaktives Risikomanagement, transparente Kommunikation und technisch robuste KI-Systeme werden Risiken für Gesundheit, Sicherheit und Grundrechte minimiert. Dies stärkt zugleich das **Vertrauen** von Kunden, Mitarbeitern und der Öffentlichkeit in KI-Anwendungen des Unternehmens [2] [3].
- **Innovationsspielraum erhalten:** Die Umsetzung der Verordnung soll so gestaltet werden, dass **kreative Freiheiten** und Innovation nicht unnötig eingeschränkt werden. Besonders Künstler:innen und Kreative sollen KI weiter nutzen können, während ihre Rechte (z. B. geistiges Eigentum) gewahrt bleiben.

- **Pragmatischer Leitfaden:** Durch klare Schritte, Beispiele und Werkzeuge (z. B. Checklisten) wird die Umsetzung praxisnah erleichtert. Insbesondere **KMU und Einzelunternehmer** profitieren von Tipps zur schlanken Integration der Compliance-Maßnahmen in bestehende Abläufe. Die Verordnung selbst enthält Erleichterungen für KMU (z. B. Zugang zu regulatorischen Sandkästen, reduzierte Gebühren und vereinfachte Dokumentationsvorlagen) [4] [5].

Mit diesem Zielbild können Unternehmen proaktiv die Weichen stellen, um die EU-KI-Verordnung nicht als Hürde, sondern als Chance für **qualitativ hochwertige und vertrauenswürdige KI** zu nutzen.

Marktanalyse & Regulatorische Einordnung

Hintergrund der EU-KI-Verordnung

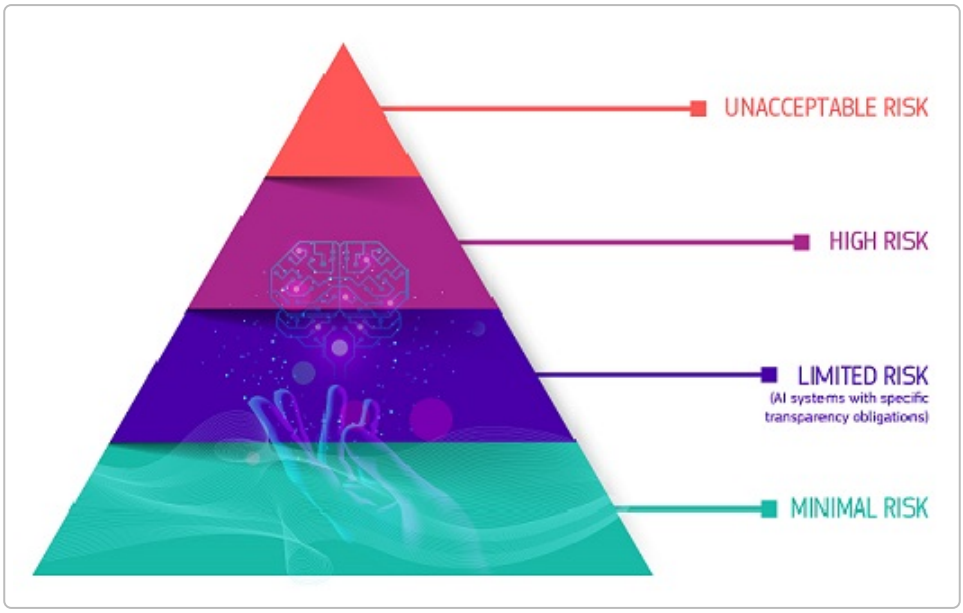
Die EU-KI-Verordnung (AI Act) trat am 1. August 2024 in Kraft und wird nach einer Übergangsfrist ab 2026 weitgehend verpflichtend gelten [6]. Sie stellt den weltweit ersten horizontalen Rechtsrahmen für KI dar [7]. Das Gesetz wurde als Reaktion auf das rapide Wachstum von KI-Systemen und deren potenzielle Risiken für Verbraucher und Grundrechte entwickelt [8] [9]. Die Verordnung verfolgt einen **risikobasierten Ansatz**: Anstatt jede KI-Technologie gleich zu behandeln, werden Anforderungen abgestuft nach dem **Gefährdungspotenzial** des jeweiligen KI-Einsatzes festgelegt [10]. Dies soll gewährleisten, dass **innovative Anwendungen** nicht durch unnötige Bürokratie gebremst werden, während **sensible Einsatzfelder** streng reguliert werden.

Geltungsbereich: Die Regelungen betreffen *nahezu alle Unternehmen*, die KI-Systeme in der EU **entwickeln, in Verkehr bringen oder nutzen** [11]. Dazu zählen KI-Softwareanbieter, Integratoren, Händler und auch die rein **nutzenden Unternehmen**, sofern sie KI in ihren Geschäftsprozessen einsetzen [11]. Auch ausländische Firmen ohne Sitz in der EU fallen unter die Verordnung, wenn sie KI-Systeme in der EU anbieten [12]. Bestimmte Bereiche sind allerdings ausgenommen, z. B. **ausschließlich private und nicht-kommerzielle KI-Nutzung**, militärische Anwendungen und Forschungsprojekte unter kontrollierten Bedingungen [13] [14].

Definition „KI-System“: Die Verordnung liefert eine eigene Begriffsbestimmung, die nicht jede Software erfasst. Sie orientiert sich an internationalen Definitionen und umfasst im Kern softwarebasierte Systeme, die mittels maschineller Ansätze (z. B. maschinelles Lernen, logikbasierte Ansätze, statistische Ansätze) aus Daten Schlussfolgerungen ziehen [15]. **Regelbasierte Algorithmen** einfacher Art ohne Lernfähigkeit fallen tendenziell nicht darunter. Unternehmen sollten prüfen, welche ihrer Anwendungen unter diese Definition fallen – viele moderne Tools (wie z. B. **generative KI**, Empfehlungssysteme, vorausschauende Analytik) gelten als KI-Systeme im Sinne des Gesetzes.

Risikoklassifizierung von KI-Systemen

Die KI-Verordnung teilt KI-Anwendungen in **vier Risikostufen** ein, verbunden mit abgestuften Pflichten [16] [17]. Diese Pyramide bildet das Herz des Gesetzes, da je nach Risikoklasse unterschiedliche Anforderungen gelten:



Risikobasierter Ansatz der EU-KI-Verordnung: KI-Systeme werden in vier Kategorien eingestuft – von minimalem bis unannehmbarem Risiko. Die regulatorischen Pflichten nehmen von unten nach oben zu [18] [3].

- **Minimales Risiko:** Die unterste Stufe umfasst die meisten KI-Systeme des Alltags, die **kaum Risiken** für Nutzer mit sich bringen (Beispiele: Spamfilter, KI in Videospielen) [18]. Für diese Systeme sieht die Verordnung *keine spezifischen Auflagen* vor. Die allgemeine Produktsicherheit und bestehende Gesetze (z. B. **DSGVO** bei Personendaten) gelten natürlich weiterhin, aber es gibt keine zusätzlichen KI-spezifischen Pflichten. Unternehmen können freiwillig **Verhaltenskodizes** oder interne Richtlinien anwenden, um Best Practices zu etablieren [18].
- **Begrenztes Risiko (transparenzpflichtig):** In diese Kategorie fallen KI-Systeme, die an sich nicht hochriskant sind, aber **Transparenzrisiken** bergen [19]. Typische Beispiele sind **Chatbots**, mit denen Nutzer interagieren, oder **generative KI**, die Inhalte erstellt [20]. Hier schreibt das Gesetz *besondere Transparenzpflichten* vor: Nutzer müssen klar darüber informiert werden, dass sie es mit einer KI zu tun haben [21]. Ebenso müssen **KI-generierte Inhalte** in bestimmten Fällen als solche kenntlich gemacht werden – z. B. **Deepfake-Bilder oder -Videos** müssen eindeutig als KI-Erzeugnisse gekennzeichnet sein [22] [23]. Diese Kennzeichnungspflichten sollen Täuschung und Manipulation verhindern, tangieren aber keine weitergehenden Anforderungen. Unternehmen sollten jedoch intern auch für begrenzte KI-Systeme Prozesse etablieren, um die Einhaltung der Transparenz sicherzustellen (siehe Abschnitt *Transparenz- und Kennzeichnungspflichten*).
- **Hohes Risiko:** Diese Kategorie betrifft KI-Systeme, deren Einsatz **signifikante Auswirkungen** auf die Lebensbereiche von Menschen haben kann – etwa auf Gesundheit, Sicherheit oder Grundrechte [24] [25]. Beispiele (Annex III der Verordnung) sind u. a. KI in **kritischen Infrastrukturen** (z. B. Verkehrssteuerung), im **Bildungs- und Prüfungswesen** (Scoring von Tests), in der **Personalverwaltung** (z. B. automatisierte Bewerberauswahl), bei der **Kreditvergabe** oder in der **medizinischen Diagnose** [26] [27]. Für Hochrisiko-KI-Systeme gelten *strenge Auflagen*: Der Anbieter muss ein umfassendes **Risikomanagementsystem** durchlaufen (inklusive Risikoanalysen und -minderungsmaßnahmen) und **hochwertige Trainings- und Testdatensätze** einsetzen, um Diskriminierung zu minimieren [28]. Weiterhin sind **Protokollierungs- und Dokumentationspflichten** einzuhalten, es müssen **klare Informationen** und Gebrauchsanweisungen an die Nutzer (Betreiber) gegeben werden, und es ist eine angemessene **menschliche Aufsicht** sicherzustellen [2]. Auch Anforderungen an **Genauigkeit, Robustheit und Cybersicherheit** des Systems sind zu erfüllen [28]. Vor dem

Inverkehrbringen muss ein **Konformitätsbewertungsverfahren** durchlaufen und eine **CE-Kennzeichnung** angebracht werden (analog zu CE-Kennzeichen bei z. B. Maschinen oder Elektronik) [29] [30]. Details dazu folgen im Abschnitt *Technische Dokumentation und Konformitätsbewertung*.

- **Unannehmbares (verbotenes) Risiko:** Diese Spitze der Pyramide umfasst KI-Anwendungen, die eine **klare Bedrohung** für die Sicherheit, Lebensgrundlagen oder Grundrechte darstellen [31]. Sie sind **verboten** und dürfen *weder entwickelt noch eingesetzt* werden [3]. Konkret nennt die Verordnung acht verbotene KI-Praktiken [32] [33], darunter etwa **Manipulation von Menschen** durch subliminale Techniken, **Ausnutzung vulnerabler Gruppen** (z. B. von Kindern, Kranken) zu ihrem Nachteil [32], **allgemeine Social-Scoring-Systeme** nach chinesischem Vorbild [3], oder bestimmte Formen von **biometrischer Überwachung** in der Öffentlichkeit (insb. *Echtzeit*-Gesichtserkennung durch Strafverfolger) [34]. Unternehmen müssen sicherstellen, dass sie derartige Anwendungen weder in der Produktentwicklung anstreben noch von Dritten einkaufen – auch nicht als Test. Sollte ein ursprünglich erlaubtes System durch neuen Kontext in diesen Bereich rutschen, ist ein sofortiger **Stopp** geboten.

Ergänzend zu diesen Kategorien für spezielle Anwendungsfälle führt die Verordnung den Begriff **„KI-Modelle für allgemeine Zwecke“** ein (auch *General Purpose AI*, darunter fallen z. B. große **generative Modelle** wie ChatGPT, DALL·E, Stable Diffusion etc.). Diese Modelle sind oft *nicht auf einen einzigen Zweck beschränkt* und können in vielen Kontexten eingesetzt werden. Für ihre Entwickler (Anbieter) gelten **zusätzliche Pflichten** (siehe Abschnitt *Umsetzungsstrategie*), u. a. in Bezug auf **Transparenz, Risikobewertung und Urheberrechtsschutz** [35] [35]. Das Gesetz unterscheidet hierbei normale und *systemisch riskante* GPAI-Modelle – letztere sind besonders leistungsfähige Modelle mit potentiell **großflächigen Auswirkungen**, für die ggf. verstärkte Aufsicht vorgesehen ist [36]. Diese Bestimmungen treten 2025 in Kraft und sollen gewährleisten, dass auch die Basistechnologien (die oft im Hintergrund von vielen Diensten laufen) **verantwortungsvoll** entwickelt werden [37].

Auswirkungen auf Künstlerische und Kreative Berufe

Ein besonderer Fokus liegt auf den **Auswirkungen für Künstler:innen, Designer, Autoren und andere Kreativschaffende**, da diese Gruppe durch generative KI-Technologien sowohl **profitiert** als auch **Herausforderungen** erfährt [38]. Generative KI-Modelle können z. B. Bilder, Musik oder Texte produzieren und damit kreative Prozesse beschleunigen. Gleichzeitig nutzen solche Modelle oft bestehende Werke als Trainingsgrundlage, was Bedenken hinsichtlich des **Schutzes geistigen Eigentums** auslöst [39] [9].

Die KI-Verordnung adressiert diese Thematik an mehreren Stellen:

- **Transparenz für KI-Inhalte:** Kreative, die generative KI einsetzen (etwa um Grafiken oder Texte zu erstellen), müssen künftig in bestimmten Fällen offenlegen, dass es sich um KI-generierte Inhalte handelt. Insbesondere wenn Werke veröffentlicht werden, die echten Personen oder Werken ähneln (Stichwort **Deepfake-Kunst**), besteht eine Kennzeichnungspflicht [22] [23]. Beispiel: Ein*e Digitalkünstler*in erstellt mittels KI ein Musikvideo mit dem Gesicht einer realen Person – dieses Video muss klar als künstlich erzeugt markiert werden, um Verwechslungen zu vermeiden. Für rein kreative, abstrakte Werke ohne Täuschungsgefahr gibt es hingegen keine allgemeine Label-Pflicht (vgl. Abschnitt *Transparenzpflichten*). Dennoch kann es aus ethischen Gründen sinnvoll sein, **freiwillig** auf KI-Einsatz hinzuweisen, um Transparenz gegenüber Publikum und Auftraggebern herzustellen [40] [6].
- **Urheberrecht und Trainingsdaten:** Ein zentrales Anliegen von Künstler:innen ist, dass ihre geschützten Werke nicht ungefragt zum Training von KI-Modellen benutzt werden. Die Verordnung verlangt daher von Anbietern großer KI-Modelle, **Urheberrechte strikt zu**

respektieren [41] . Konkret müssen Entwickler allgemeiner KI-Modelle eine **Policy für Copyright-Compliance** implementieren und sicherstellen, dass sie etwaige **Opt-out-Verfügungen** von Rechteinhaber:innen erkennen und beachten [42] [41] . Seit 2019 können Urheber über einen Rechtsvorbehalt (z. B. in Metadaten oder per robots.txt für Websites) der automatisierten Analyse ihrer Inhalte widersprechen [43] [44] . Hat ein*e Künstler*in also z. B. ihre Bilder mit einem „nicht für KI-Training freigegeben"-Tag versehen, muss ein KI-Anbieter dafür Sorge tragen, diese Bilder *nicht* in seine Trainingsdaten aufzunehmen [45] . Zudem sind KI-Anbieter verpflichtet, eine **zusammenfassende Liste der verwendeten Trainingsdaten** zu veröffentlichen [46] . Dadurch soll für Kreative zumindest nachvollziehbar werden, aus welchen Quellen ein Modell „gelernt" hat – vollständige Transparenz auf Dateiebene ist zwar nicht garantiert, aber Kategorien oder große Datensätze werden offengelegt. Dies versetzt Urheber in die Lage, festzustellen, ob z. B. ihr Portfolio Teil eines Trainings war, und gegebenenfalls Ansprüche geltend zu machen [35] [35] . Allerdings gibt es hierbei auch Kritik aus Urheber-Sicht, da eine nachträgliche Entfernung schwierig sein kann und die aktuellen EU-Copyright-Regeln (Stichwort Text-und Data-Mining-Ausnahmen) Schlupflöcher lassen [47] [35] .
- **Kreative Freiheiten vs. Regulierung:** Die Verordnung versucht, einen Ausgleich zu schaffen zwischen Reglementierung und künstlerischer Freiheit. So gelten etwa **Ausnahmen für Forschung und Kunst** bei bestimmten Verboten und Transparenzpflichten, solange keine Verletzung von Grundrechten vorliegt. Reine Kunstprojekte, die KI experimentell einsetzen, könnten unter künstlerische Freiheiten fallen – allerdings ist diese Abgrenzung noch in der Praxis zu beobachten. Künstler:innen sollten im Zweifel annehmen, dass Publikationen mit KI-Inhalten den Transparenzpflichten unterliegen, um sicher zu gehen. Gleichzeitig ist positiv zu vermerken, dass die KI-Verordnung *keine Zensur von Inhalten* vornimmt – sie schreibt z. B. nicht vor, welche Kunststile erlaubt sind, sondern nur **wie** KI-Kunst im Umgang transparent und sicher gestaltet sein muss.
- **Neue Marktchancen:** Für die Kreativwirtschaft entstehen durch die Regulierung auch Chancen. So könnte ein Markt für **lizenzierte Trainingsdaten** oder für **zertifizierte „ethical AI"-Tools** entstehen, von dem Künstler profitieren – etwa wenn Plattformen garantieren, nur freigegebene Werke in KI-Trainings zu verwenden. Künstler selbst können mit *KI-gestützter Kreativität* neue Geschäftsmodelle entwickeln (personalisierte Inhalte, interaktive Medienkunst), wobei die Einhaltung der Regeln einen **Qualitäts- und Vertrauensvorteil** verschafft. Zudem klärt die Rechtslage zunehmend Fragen (wie das Thema Urheberrecht an KI-Werken [48]), was langfristig zu mehr Rechtssicherheit im kreativen Schaffen mit KI führt.

Fazit für Kreative: Die KI-Verordnung schützt primär Verbraucher und Grundrechte [8] – für Kreative bietet sie (noch) keine umfassende Lösung aller Urheberrechtsprobleme, aber zumindest **Ansatzpunkte für fairen Umgang** mit ihren Werken. Künstler:innen und kreative Unternehmen sollten die Entwicklung begleiten, ihre Werke ggf. kennzeichnen (Opt-out) und bei KI-Einsatz transparent sein. Im nächsten Abschnitt wird dargestellt, wie Unternehmen – einschließlich Kreativbetrieben – die verschiedenen Anforderungen praktisch umsetzen können.

Umsetzungsstrategie für Unternehmen

In diesem Kapitel wird beschrieben, **wie** Unternehmen die Vorgaben der KI-Verordnung konkret erfüllen können. Die Strategie ist modular aufgebaut, sodass sie für **verschiedene Unternehmensgrößen und Branchen** passt. Einzelne Schritte bzw. Maßnahmen sollten je nach Risikoprofil des Unternehmens angepasst werden. Für jeden Aspekt der Verordnung (Risikoklassifizierung, Transparenz, Datenschutz, Dokumentation, Monitoring, Aufsicht/Robustheit) werden Maßnahmen aufgezeigt.

Zunächst sollte jedes Unternehmen ein internes **KI-Compliance-Team** oder zumindest eine verantwortliche Person bestimmen, die die Umsetzung koordiniert. Bei kleinen Unternehmen kann dies der Geschäftsführende selbst oder z. B. der Datenschutzbeauftragte in Doppelfunktion übernehmen. Wichtig ist, dass **Know-how zu KI und Regulierung** gebündelt wird, um die folgenden Schritte systematisch anzugehen.

1. Risikoklassifizierung der eingesetzten KI-Systeme

Warum wichtig: Die Risikoklassifizierung ist der Ausgangspunkt aller weiteren Maßnahmen – sie bestimmt, welche Pflichten im Einzelfall greifen. Unternehmen müssen daher zunächst **Inventur** machen: *Welche KI-Systeme nutzen oder entwickeln wir?* Jedes identifizierte System ist einer der vier Risikostufen (siehe oben) zuzuordnen.

Vorgehen:

- **KI-Inventarliste erstellen:** Alle Anwendungen, Dienste oder Komponenten mit KI-Funktion identifizieren. Dazu gehören offensichtlich KI-basierte Tools (z. B. Machine-Learning-Modelle für Vorhersagen), aber auch zugekaufte Lösungen, die KI nutzen (z. B. eine HR-Software mit CV-Screening-Algorithmus, ein Marketing-Tool mit KI-Textgenerator). Wichtig: Auch Cloud-Dienste von Drittanbietern, die KI-Funktionen bieten, erfassen, sofern sie in eigenen Prozessen genutzt werden.
- **Abgleich mit KI-Begriffsdefinition:** Prüfen, ob die Anwendung unter die KI-Definition der Verordnung fällt. Einfache regelbasierte Software oder BI-Analysen ohne maschinelles Lernen könnten ausgenommen sein [15]. Im Zweifel kann man annehmen, dass alles, was gemeinhin als „AI“ vermarktet wird oder *selbstlernende* bzw. komplexe algorithmische Funktionen hat, unter das Gesetz fällt.
- **Bestimmung des Verwendungszwecks und Kontextes:** Für jedes KI-System klären, *wozu* es eingesetzt wird und *wer* bzw. *was* davon betroffen ist. Beispielsweise kann eine Gesichtserkennungs-KI zur Zugangskontrolle am Firmengebäude ein anderes Risikoprofil haben als dieselbe Technologie im öffentlichen Raum durch Behörden. Kontext und Zweck entscheiden über die Einstufung als Hochrisiko oder nicht [49] [17].
- **Risikoklasse zuordnen:** Anhand der Inventarliste und der **Annex-III-Liste** der Verordnung (dort sind Hochrisiko-Anwendungsfelder aufgezählt) kategorisieren:
- Wenn das System in eine der **Hochrisiko-Anwendungen** fällt (z. B. medizinische Diagnosesoftware, Algorithmen zur Kreditwürdigkeitsprüfung, sicherheitskritische Fertigungssteuerung), **Einstufung als hochriskant**.
- Wenn das System eine **verbotene Praxis** umsetzt (siehe Liste der unannehmbaren Risiken, z. B. Social Scoring oder manipulative KI), **sofort stoppen** – gar nicht erst einsetzen oder entwickeln. Dies dürfte selten auf normale Unternehmen zutreffen, eher auf spezielle Fälle (z. B. wäre ein Marketing-Tool, das Kunden unmerklich subliminal beeinflusst, unzulässig).
- Wenn weder Hochrisiko noch verboten, prüfen, ob **Transparenzpflichten** greifen: Interagiert die KI direkt mit Personen? Generiert sie Inhalte, die echt wirken könnten? Wenn ja, **begrenzte Risikoklasse (Transparenz-Pflichten)** annehmen. Andernfalls gilt **minimales Risiko**.
- **Dokumentation der Einstufung:** Es empfiehlt sich, für jedes KI-System kurz zu notieren, warum man es in Klasse X eingeordnet hat (z. B. *„CV-Analysetool für Recruiting – Hochrisiko gem. KI-VO Annex III (Beschäftigung und Personalverwaltung)“* oder *„Chatbot auf Website – begrenztes Risiko, Transparenzpflicht“*). Diese Notizen helfen bei internen Freigabeprozessen und sind wertvoll, falls eine Behörde später Nachfragen hat.

Besonderheit kleine Unternehmen: Wenn nur **Standardsoftware mit KI** genutzt wird (z. B. Office-Tools mit KI-Assistenten), ist die Einstufung meist **minimales Risiko**. Dennoch sollte man auch als kleines

Unternehmen einen Überblick haben, wo KI im Spiel ist. Für viele KMU wird das Ergebnis der Klassifizierung sein, dass **keine Hochrisiko-Systeme** vorliegen – was den Umsetzungsaufwand deutlich reduziert. Falls doch, kann externe Beratung bei der Einstufung sinnvoll sein, da hier dann komplexere Pflichten folgen.

2. Transparenz- und Kennzeichnungspflichten umsetzen

Was ist gefordert: Für KI-Systeme der *begrenzten Risikokategorie* schreibt die Verordnung bestimmte Transparenzmaßnahmen vor [21]. Ziel ist es, **Nutzer oder Betroffene nicht im Unklaren zu lassen**, wenn KI involviert ist, um informierte Entscheidungen zu ermöglichen und Vertrauen zu schaffen [50]. Konkret gibt es drei typische Fälle:

- **KI-Interaktion:** Wenn ein Mensch mit einem KI-System **interagiert**, muss er/sie darauf hingewiesen werden, dass es sich um KI handelt und kein menschliches Gegenüber [21]. Beispiel: Ein Chatbot im Kundenservice muss sich als „virtueller Assistent" oder Ähnliches zu erkennen geben.
- **Generative KI-Inhalte:** Inhalte (Text, Bild, Audio, Video), die mithilfe von KI erzeugt wurden, **müssen als KI-generiert kenntlich** gemacht werden, *wenn* die Gefahr besteht, dass sie sonst für von Menschen geschaffen gehalten würden [51]. Besonders relevant ist dies bei **synthetischen Medien** wie realistisch wirkenden KI-Bildern oder -Stimmen. Die Verordnung nennt explizit **Deepfakes**, die klar markiert werden müssen [22] [23]. Ein einfacher Hinweis wie „Dieses Bild wurde mit KI erstellt" oder ein sichtbares Wasserzeichen genügt, solange es für einen durchschnittlichen Betrachter verständlich ist [52]. Bei Texten wird empfohlen, zumindest im Impressum oder Begleittext anzugeben, dass KI genutzt wurde – auch wenn nicht in jedem Fall eine rechtliche Pflicht besteht [6].
- **Emotionserkennung/Biometrik:** Falls KI-Systeme eingesetzt werden, um Emotionen, Gesichtsausdrücke oder biometrische Merkmale auszuwerten (z. B. Gesichtskamera zur Stimmungserkennung), sind ebenfalls **Transparenzhinweise** gegenüber den beobachteten Personen erforderlich. Dieser Fall ist hochsensibel und oft als Hochrisiko einzustufen (z. B. Echtzeit-Biometrie wäre verboten bzw. genehmigungspflichtig). In weniger strengen Fällen (z. B. Gefühlsanalyse bei einer freiwilligen Werbeaktion) muss zumindest klar sein, dass eine KI solche Daten verarbeitet.

Maßnahmen zur Umsetzung:

- **Nutzerinformation bereitstellen:** In allen Interfaces, wo Endnutzer mit KI zu tun haben, einen gut sichtbaren Hinweis einbauen. Beispiele: Begrüßungsnachricht des Chatbots: *„Ich bin ein KI-gestütztes Assistenzsystem…"*; Pop-up bei einem KI-Bildergenerator: *„Bild automatisch generiert durch KI"*. Wichtig ist die Verständlichkeit: keine technischen Fachbegriffe, sondern klare Sprache (ggf. mehrsprachig, je nach Zielgruppe).
- **Kennzeichnung von Inhalten:** Für KI-generierte Bilder/Grafiken kann man kleine Wasserzeichen oder Fußnoten anbringen [53]. In Social Media Kontext eignen sich Hashtags wie `#KI-generiert` oder entsprechende Labels, die einige Plattformen bereits anbieten [54]. Unternehmen sollten interne **Styleguides** entwickeln, wann und wie KI-Inhalte zu markieren sind – z. B. alle Produktfotos, die aus KI stammen, erhalten im Dateinamen oder in der Bildunterschrift einen Standardhinweis. Für Audio/Video-Inhalte kann in den Metadaten oder im Abspann eine Notiz „KI-generiert" eingefügt werden.
- **Mitarbeiter schulen:** Alle Mitarbeiter, die Texte, Bilder oder andere Inhalte veröffentlichen, sollten sensibilisiert werden, inwiefern KI bei der Erstellung beteiligt war und wann eine Kennzeichnung erfolgen muss. Oft wissen z. B. Marketing-Teams gar nicht, dass ein Stock-Foto

durch KI entstanden ist – hier hilft Kommunikation mit Dienstleistern oder Agenturen. Lieber im Zweifel einen Transparenzhinweis geben, auch wenn nicht 100% sicher.

- **Systeme zur Erkennung einsetzen:** Perspektivisch könnten technische Lösungen helfen, KI-Inhalte automatisch zu erkennen (Stichwort **KI-Detektoren**). Einige große Plattformen wie Meta arbeiten an automatischer Kennzeichnung von KI-Bildern [55]. Unternehmen sollten solche Tools beobachten und ggf. integrieren, um die Einhaltung zu erleichtern.
- **Dokumentation der Maßnahme:** Festhalten, welche KI-Systeme einer Transparenzpflicht unterlagen und wie das umgesetzt wurde (z. B. *„Chatbot X – Hinweis im Header eingefügt am 01.01.2025“*). Dies kann Teil der technischen Dokumentation oder eines internen **Transparenzregisters** sein.

Besonderer Tipp für Kreative: Wenn KI als *Assistenz* im Schaffensprozess genutzt wurde (z. B. KI half beim Entwurf, das Endergebnis ist aber stark von menschlicher Hand geprägt), muss man es **nicht** explizit deklarieren [6]. Dennoch kann es aus Transparenzgründen sinnvoll sein, den KI-Anteil offenzulegen – etwa gegenüber Auftraggebern, um Erwartungen zu managen (z. B. in welchem Maße das Werk originär ist). In jedem Fall sollte vermieden werden, KI-erschaffene Werke als vollständig eigene menschliche Schöpfung auszugeben, da dies rechtliche Unsicherheiten (Urheberrecht) birgt und dem Transparenzgebot des AI Act widerspricht.

3. Datenschutz und Daten-Governance sicherstellen

Was ist gefordert: Die KI-Verordnung legt großen Wert auf **qualitativ hochwertige, rechtmäßig erhobene und verwaltete Daten** für KI-Systeme [28] [56]. Dies schließt den Datenschutz im Sinne der DSGVO sowie Maßnahmen gegen Verzerrungen (Bias) ein. Artikel 10 AI Act fordert, dass Trainings-, Validierungs- und Testdaten *relevant, repräsentativ, fehlerfrei und möglichst vollständig* sein müssen [57]. Zudem müssen Datensätze die **statistischen Merkmale** der betroffenen Bevölkerungsgruppen angemessen abbilden, um Diskriminierung vorzubeugen [56]. Praktisch heißt das: Unternehmen brauchen ein **Daten-Governance-Konzept** für alle KI-bezogenen Daten.

Maßnahmen zur Umsetzung:

- **DSGVO-Compliance als Grundlage:** Falls KI-Systeme mit *personenbezogenen Daten* arbeiten (z. B. Kundendaten in einem ML-Modell), muss die **DSGVO** strikt eingehalten werden. Das bedeutet u. a.:
- Rechtsgrundlage prüfen (Einwilligung der Betroffenen, Vertragserfüllung, berechtigtes Interesse etc. – je nach Anwendungsfall) [58] [59]. Ohne gültige Grundlage dürfen solche Daten nicht in KI-Modelle fließen. Besonders kritisch: Daten von Dritten, die evtl. über öffentliche Quellen bezogen wurden (Web Scraping) – hier ist meist keine Einwilligung gegeben.
- Datentransfers in Drittstaaten: Viele KI-Dienste (Cloud-Services, API für ML) senden Daten in die USA oder andere Länder [60] [61]. Hier müssen Unternehmen sicherstellen, dass ein zulässiger Transfermechanismus besteht (Standardvertragsklauseln, Angemessenheitsbeschluss etc.), sonst verstößt die Nutzung gegen Datenschutzrecht – und indirekt auch gegen die **Daten-Governance-Pflicht**.
- Minimaldatenspeicherung und Löschfristen: Keine unnötigen personenbezogenen Daten länger speichern als nötig.
- Betroffenenrechte: Prozesse vorhalten, um Auskunft, Löschung oder Korrektur von personenbezogenen Trainingsdaten umzusetzen, falls jemand das verlangt. (Dies ist herausfordernd – aber zumindest konzeptionell sollten Unternehmen darauf vorbereitet sein, auch wenn es in ML-Modellen praktisch schwierig ist.)
- **Datenqualität und Bias-Checks:** Für KI-Trainingsdaten (sowie Testdaten) Mechanismen einführen, die Qualität sichern:

- **Datenbereinigung:** Vor Nutzung sollten Datensätze auf offensichtliche Fehler, Duplikate oder irrelevante Einträge geprüft und bereinigt werden.
- **Repräsentativität prüfen:** Enthalten die Daten alle relevanten Gruppen, oder sind bestimmte Altersgruppen, Geschlechter, Ethnien etc. unterrepräsentiert? Wenn ja, überlegen, ob das die Anwendung verzerrt (Bias). Ggf. zusätzliche Datenpunkte sammeln oder **synthetische Daten** ergänzen, um Verzerrungen auszugleichen. Bei kleinen Unternehmen kann schon das Bewusstsein helfen – z. B. bei einem lokal trainierten Sprachmodell darauf achten, verschiedene Dialekte oder Sprechweisen einzubeziehen, falls relevant.
- **Bias-Metriken einsetzen:** Es gibt Open-Source-Toolkits (wie IBM AI Fairness 360, Google What-If-Tool u.a.), die Datensätze und Modelle auf Verzerrungen analysieren können. Solche Tools sollte man – Ressourcen vorausgesetzt – einsetzen, insbesondere bei kritischeren Anwendungen (z. B. HR, Kredit).
- **Dokumentation von Datenquellen:** Für die technische Dokumentation (s. u.) muss ohnehin erfasst werden, woher die Trainingsdaten stammen. Empfehlenswert ist eine Tabelle oder ein Datenkatalog mit Angaben: Quelle (eigene Erhebung, öffentlich, Drittanbieter), Umfang, ggf. Anteil sensibler Daten, Genehmigungen/Lizenzen (gerade wichtig bei *urheberrechtlich geschütztem Material*!).
- **Opt-Out und Lizenzen beachten:** Wie im Abschnitt Kreative beschrieben, müssen Unternehmen (insb. Anbieter von KI-Modellen) darauf achten, keine urheberrechtlich geschützten Daten unerlaubt zu verwenden [42]. Falls man z. B. öffentliche Daten aus dem Internet scrapt, sollte zuvor geprüft werden, ob Rechte vorbehalten wurden (etwa durch **robots.txt** oder in AGB der Website). Im Zweifel lieber auf solche Daten verzichten oder eine Nutzungserlaubnis einholen. Es gibt bereits Content-Plattformen, die bestimmte Daten für KI frei lizenzieren – solche **legitimierten Datenquellen** sind vorzuziehen.
- **Daten-Governance-Prozess etablieren:** Größere Firmen sollten einen formalen Prozess definieren, z. B. in Form eines **Daten-Governance-Boards** oder zumindest eines Verantwortlichen:
- Klare Rollen: Wer ist Data Owner, wer kümmert sich um Datenqualität?
- Richtlinien: z. B. „Für jedes neue KI-Projekt ist ein Datasheet zu erstellen, das die oben genannten Punkte (Qualität, Bias etc.) adressiert."
- Periodische Überprüfung: Daten verändern sich über die Zeit; regelmäßige Audits der Daten und Modelle (z. B. jährlich) können sicherstellen, dass die KI nicht durch Drift oder neue Verzerrungen unerkannt problematisch wird.
- **Schutz besonderer Daten:** In manchen Fällen erlaubt die KI-Verordnung sogar die Verarbeitung *besonders geschützter personenbezogener Daten* (z. B. zu Ethnie, Gesundheit) – allerdings **ausschließlich**, um Bias zu erkennen und zu mindern [57]. Falls ein Unternehmen dies tut (etwa um zu prüfen, ob ein Modell bestimmte Gruppen diskriminiert), muss es strenge Zugriffskontrollen und Sicherheitsmaßnahmen haben. Solche sensiblen Analysedaten sollten nach der Auswertung wieder gelöscht oder anonymisiert werden.

Kurz gesagt: **Datendisziplin** ist unerlässlich. Unternehmen, die bisher unbedarft „alle verfügbaren Daten in die KI kippen", müssen umdenken und strukturierter vorgehen. Die Belohnung sind **verlässlichere Modelle** und weniger rechtliche Risiken. Zudem decken sich viele dieser Anforderungen mit guter Praxis in der Datenwissenschaft (Stichwort *Data Cleaning*, *Responsible AI*), was letztlich auch die Modellperformance verbessern kann.

4. Technische Dokumentation und Konformitätsbewertung

Was ist gefordert: Für **hochriskante KI-Systeme** verlangt die Verordnung eine ausführliche **technische Dokumentation** sowie eine **Konformitätsbewertung vor dem Inverkehrbringen** [28] [2]. Ähnlich wie bei Medizinprodukten oder Maschinen muss der Anbieter nachweisen, dass sein KI-System

alle Anforderungen erfüllt, und dies in einer **EU-Konformitätserklärung** bestätigen [62]. Erst dann darf das System mit einem **CE-Kennzeichen** vertrieben werden [63]. Betreiber (Nutzer) von Hochrisiko-KI haben ebenfalls bestimmte Dokumentations- und Meldepflichten im Betrieb (dazu im nächsten Abschnitt mehr).

Maßnahmen zur Umsetzung (für Anbieter/Entwickler von KI-Systemen):

- **Technical File erstellen:** Sobald klar ist, dass ein KI-System als hochriskant eingestuft wurde (siehe Schritt 1), sollte ein *„Technical File"* angelegt werden, analog zur Technischen Dokumentation bei anderen CE-Produkten. Darin sollten mindestens folgende Inhalte abgedeckt sein (vgl. Anhänge IV und XI der KI-Verordnung):
- **Systembeschreibung:** Was macht das KI-System, wofür ist es bestimmt, welche Grenzen hat es? (Beispiel: *„KI-Software zur Diagnostik, unterstützt Radiologen bei der Erkennung von Tumoren auf MRT-Bildern. Nicht zur autonomen Diagnose ohne ärztliche Abnahme vorgesehen."*)
- **Funktionsprinzip:** Beschreibung der KI-Methode (Algorithmus, Modelltyp), Trainingsverfahren, Eingabedaten und erwartete Ausgabe. Hier darf man durchaus technisch werden, inkl. Modellarchitektur und Parametern – soweit es fürs Verständnis nötig ist.
- **Trainings- und Testdatenbeschreibung:** Quellen und Eigenschaften der Daten (siehe Daten-Governance oben). Evtl. Statistiken über Daten (Größe, Verteilung) und bekannte Limitationen (z. B. „Datensatz enthält überwiegend Bilder aus europäischen Krankenhäusern, andere Ethnien könnten unterrepräsentiert sein").
- **Risikomanagement-Nachweis:** Ein Dokument oder Abschnitt, das den **Risikomanagement-Prozess** nach Artikel 9 belegt. Dazu gehört eine Liste identifizierter Risiken (z. B. Fehlalarme, falsche Negative, Bias gegen Gruppe X, Ausfälle bei bestimmten Lichtverhältnissen, etc.) sowie die jeweils ergriffenen Gegenmaßnahmen. Eine Art FMEA (Failure Mode and Effects Analysis) für KI kann hier sinnvoll sein.
- **Konformität mit Anforderungen:** Auflistung, wie das System die konkret geltenden Anforderungen aus der Verordnung einhält: z. B. *„Datenqualität: erfüllt, da Trainingsdaten manuell verifiziert und bereinigt [56]; Transparenz: Bedienungsanleitung enthält alle Infos für Nutzer [2]; Cybersicherheit: regelmäßige Penetration-Tests durchgeführt."* Falls es einschlägige harmonisierte **Standards** gibt, kann man sich darauf beziehen (bis 2025/26 werden vermutlich EU-Standards oder ISO-Normen für KI herauskommen). Die Einhaltung solcher Standards schafft die **Vermutung der Konformität**, was das Verfahren erleichtert.
- **Testergebnisse:** Ergebnisse von Validierungs- und Verifizierungsverfahren, z. B. Genauigkeitsraten, Fehlerraten, Robustheitstests (z. B. wie reagiert das System auf Rauschen oder ungewöhnliche Eingaben) [28]. Auch Performance-Metriken nach relevanten Standards (z. B. ROC-Kurven für Klassifikatoren) können hier hinein.
- **Logging und Monitoring:** Beschreibung der Protokollierungsfunktionen (Artikel 12 fordert, dass Hochrisiko-KI bestimmte Logs aufzeichnet). Notieren, welche Events geloggt werden und wie lange gespeichert [64] (gesetzlich mindestens 6 Monate im Einsatz) – etwa Entscheidungsprotokolle, Parameteränderungen etc.
- **Gebrauchsanweisung und Infos für Nutzer:** Kopie oder Entwurf der Informationsmaterialien, die dem Kunden/Betreiber mitgegeben werden (Artikel 13). Darin müssen u. a. enthalten sein: Zweck des Systems, Leistung, erforderliche Datenqualität der Inputdaten, bekannte Risiken/Limitierungen, Anleitung zur menschlichen Überwachung, Wartungshinweise, was im Falle von Fehlfunktionen zu tun ist [2]. Praktisch entspricht das einem Benutzerhandbuch mit speziellen KI-Hinweisen.

- **Möglichst: Zusammenfassung für Behörden:** Es kann helfen, zusätzlich eine nicht-vertrauliche Zusammenfassung bereitzustellen, die man z. B. einer Behörde oder dem AI Office auf Anfrage geben könnte. Dies ist besonders für kleinere Anbieter sinnvoll, damit man im Fall der Fälle

schnell liefern kann, ohne Geschäftsgeheimnisse komplett offenlegen zu müssen. (Die Verordnung verlangt zwar im Zweifel volle Einsicht, aber eine vorgefertigte Zusammenfassung schafft Vertrauen und spart Zeit.)

- **Interne Kontrolle vs. externe Prüfung:** Prüfen Sie, welches *Konformitätsbewertungsverfahren* zutrifft (Artikel 43 ff.). Viele Hochrisiko-Systeme können über **interne Kontrolle** selbst zertifiziert werden (d.h. der Anbieter erklärt eigenverantwortlich die Konformität) [65]. In bestimmten Fällen (etwa biometrische Identifikationssysteme) ist jedoch eine **Benannte Stelle** einzuschalten, die das System prüft und zertifiziert [66]. Als Unternehmen sollten Sie frühzeitig klären, ob Sie einen externen Zertifizierer brauchen – die **Notified Bodies** müssen erst benannt werden und könnten Auslastung haben. Wenn ja: Budget und Zeit für diesen Prozess einplanen, Angebote von Prüfstellen einholen. Wenn nein: sicherstellen, dass die technische Dokumentation so robust ist, dass sie einer behördlichen Überprüfung standhält.

- **EU-Konformitätserklärung ausstellen:** Sobald alle Anforderungen erfüllt und dokumentiert sind, erstellt der Anbieter die **EU-Konformitätserklärung** (eine formale Erklärung ähnlich wie bei CE-Konformität, siehe Anhang V der Verordnung) [62]. Darin wird erklärt, dass das KI-System die Verordnung einhält, unter Angabe von Produkt, Anbieter, ggf. Referenzen zu Standards, und – falls zutreffend – der benannten Stelle, die beteiligt war. Diese Erklärung muss *jedem Hochrisiko-KI-System beigefügt* werden (z. B. als Teil der Doku) und bei Behördenanfragen vorgelegt werden können [67].
- **CE-Kennzeichnung anbringen:** Das AI Act schreibt vor, dass **Hochrisiko-KI-Systeme ein CE-Zeichen** tragen müssen, sobald sie die Konformität erfüllen [65]. Ist das KI-System in ein physisches Produkt integriert (z. B. ein Roboter mit KI-Komponente), wird das CE-Zeichen am Produkt oder der Verpackung angebracht wie üblich [30]. Bei reiner Software ohne physische Form kann das CE-Zeichen in digitalen Unterlagen oder der Oberfläche erscheinen. Wichtig: Die CE-Kennzeichnung signalisiert gleichzeitig die Erfüllung aller anderen einschlägigen EU-Vorschriften [68] – d.h. wenn z. B. ein KI-Medizinprodukt vorliegt, bedeutet ein CE im Kontext AI Act auch Konformität mit der Medizinprodukteverordnung (sofern anwendbar) [68].
- **Registrierung im EU-Datenbank-Register:** Nach erfolgreicher Konformitätsbewertung müssen bestimmte Hochrisiko-KI in eine **EU-Datenbank** eingetragen werden (Art. 49). Dort werden Basisinformationen öffentlich zugänglich gemacht (z. B. Name des Systems, Zweck, Anbieter), um Transparenz gegenüber Aufsichtsbehörden und der Öffentlichkeit zu erhöhen. Unternehmen sollten diese Registrierung nicht vergessen – sie ist quasi der letzte Schritt, bevor das System offiziell in den Markt geht.

Für **bestehende KI-Systeme** am Markt gilt eine Übergangsfrist: Systeme, die vor Inkrafttreten der Verordnung bereits in Betrieb waren, genießen unter Umständen Bestandsschutz bis 2026 (Artikel 54, 55). Dennoch ist es ratsam, auch laufende Produkte **nachzudokumentieren** und sukzessive auf Konformität zu bringen, um für die Zukunft gerüstet zu sein.

Hinweis für Betreiber (anwenderseitige Unternehmen): Wenn Ihr Unternehmen KI-Systeme von Drittanbietern **einkauft oder nutzt**, vergewissern Sie sich, dass diese ab 2026 eine **CE-Kennzeichnung** tragen, falls es Hochrisiko-Systeme sind [67]. Importierte KI-Systeme müssen z. B. vom Importeur auf CE und Konformitätserklärung geprüft werden [67]. Fordern Sie vom Lieferanten die nötigen Unterlagen (mindestens Konformitätserklärung, ggf. Ausschnitt aus der Dokumentation, welche Anforderungen erfüllt sind). Beziehen Sie Compliance-Klauseln in Ihre Beschaffungsverträge ein – etwa, dass der Anbieter Sie informiert, falls das Produkt ein schwerwiegendes KI-Risiko oder einen Zwischenfall verursacht (um gemeinsam reagieren zu können).

Zusammengefasst: Für Hersteller/Anbieter von KI ist die **Produkthaftung und -sicherheit** mit der KI-Verordnung in ähnlicher Weise formalisiert worden wie in anderen Industrien. Die upfront-Dokumentation mag aufwendig sein, aber sie bildet das Fundament für **vertrauenswürdige KI-Produkte** und kann intern als wertvolles Nachschlagewerk dienen. Unternehmen, die hier investieren, werden langfristig Wettbewerbsvorteile haben, da sie Qualitätsnachweise vorlegen können, wo andere noch improvisieren.

5. Meldepflichten und Marktüberwachung (Post-Market Compliance)

Was ist gefordert: Die Verantwortung des Anbieters (und auch des Betreibers) endet nicht mit dem Inverkehrbringen. Die KI-Verordnung verpflichtet dazu, **während des Betriebs** ein **Post-Market-Monitoring** durchzuführen und **schwerwiegende Vorfälle** zu melden [69] [70]. Außerdem werden Behörden stichprobenartig die Marktaufsicht führen. Für Unternehmen bedeutet das: Es muss ein Plan geben, wie man mit Problemen einer KI nach Markteinführung umgeht und wie man mit den Aufsichtsbehörden kooperiert.

Maßnahmen:

- **Post-Market-Monitoring einrichten:** Anbieter von Hochrisiko-KI müssen aktiv Informationen sammeln, wie ihr System in der Praxis performt [69]. Dazu sollten Sie:
- Kundensupport und Feedback-Kanäle speziell auch für KI-Themen öffnen. Beispielsweise könnten Sie Ihren Kunden formalisierte Möglichkeiten geben, Fehlentscheidungen oder Sicherheitsprobleme des KI-Systems zu melden.
- Technische Telemetrie nutzen: falls zulässig (datenschutzkonform), anonymisierte Nutzungsdaten auswerten, um Auffälligkeiten zu entdecken. Z. B. plötzlicher Performanceabfall, ungewöhnliche Output-Muster etc.
- Regelmäßige Reviews: In festgelegten Intervallen (z. B. vierteljährlich) die gesammelten Post-Market-Daten sichten und analysieren. Dies könnte Teil eines **Qualitätsmanagementsystems** (Artikel 17) sein, das ohnehin für Hochrisiko-Anbieter vorgeschrieben ist.
- **Meldeprozesse für Vorfälle:** Ein *„schwerwiegender Vorfall"* (serious incident) ist nach KI-VO ein Ereignis, das zu einem rechtlichen Verstoß (z. B. Grundrechtsverletzung) oder Sicherheitsproblem führt. Beispiele: Eine KI für Kreditscoring diskriminiert systematisch eine geschützte Gruppe; ein Medizin-KI-System übersieht kritische Befunde und gefährdet Patienten. Wenn ein solcher Vorfall **mit Ihrem KI-System in Zusammenhang** steht, müssen Sie dies der zuständigen Behörde **unverzüglich, spätestens innerhalb 15 Tagen** melden [71]. Bei sehr schwerwiegenden Fällen oder wenn das Problem weitverbreitet ist, sogar binnen 2 Tagen [72].
- Legen Sie intern fest, **wer diese Meldungen vornimmt** (z. B. der Compliance Officer oder Produktmanager).
- Bereiten Sie ein Template für Incident-Berichte vor, wo die nötigen Angaben schnell eingefügt werden können: Beschreibung des Vorfalls, betroffene Personen, erste Einschätzung Ursache, ergriffene Maßnahmen (z. B. Hotfix, Deaktivierung des Systems), Kontaktperson.
- Schulen Sie auch Kundenbetreuer und Techniker, Vorfälle intern **sofort zu eskalieren**, damit die 15-Tage-Frist nicht versäumt wird. Lieber eine Meldung mehr einreichen als zu wenige – auch **Betreiber** (nutzerseitige Firmen) haben eine Meldepflicht, wenn sie vermuten, dass ein Hochrisiko-KI-System zu einem ernsthaften Vorfall geführt hat [71].
- **Zusammenarbeit mit Behörden:** Die KI-Aufsicht wird voraussichtlich durch nationale Behörden erfolgen, koordiniert durch ein europäisches **AI Office** und den European AI Board. Planen Sie, wie Sie auf **Auskunftsersuchen** oder Audits reagieren. Haben Sie z. B. einen Ansprechpartner parat und die technische Dokumentation griffbereit? Halten Sie Ihre Konformitätserklärung und Registrierungsdaten aktuell.

- Sollte eine Behörde Nachbesserungen verlangen oder ein System vom Markt nehmen wollen, nehmen Sie das sehr ernst und reagieren Sie fristgerecht. Bauen Sie idealerweise schon im Vorfeld ein **Verhältnis zu lokalen Aufsichtsbehörden** auf – z. B. via Branchennetzwerke oder freiwillige Audits.
- **Rückruf- und Update-Prozesse:** Ähnlich wie man fehlerhafte physische Produkte zurückruft, braucht es einen Plan, falls Ihre KI sich als fehlerhaft herausstellt. Können Sie per Software-Update schnell beheben? Haben Sie in Verträgen geregelt, dass Kunden Updates einspielen *müssen* bei sicherheitskritischen Bugs? Im schlimmsten Fall: Wie informieren Sie Endnutzer oder die Öffentlichkeit, falls ein Problem bekannt wird? Offene Kommunikation kann hier Schäden minimieren (Stichwort PR-Strategie bei KI-Vorfällen).
- **Lernschleife schließen:** Nutzen Sie die Erkenntnisse aus dem Betrieb, um Ihre KI kontinuierlich zu verbessern. Die Verordnung will *„lebenslanges Lernen"* auch in der Compliance: d.h. aus Incidents und Monitoring-Daten lernt man für nächste Versionen (z. B. Verbesserungen an Datensätzen, Anpassung der Algorithmen). Dokumentieren Sie diese Iterationen ebenfalls, so zeigen Sie, dass Sie der Sorgfaltspflicht nachkommen.

Insbesondere Betreiber (anwenderspezifisch) sollten intern Regeln aufstellen, wann sie ein KI-System **abschalten oder außer Betrieb nehmen**, falls es auffällig wird. Z.B.: Ein Krankenhaus als Betreiber einer KI-Diagnose-Software könnte definieren, dass bei bestimmten Fehlermustern die Software solange *nicht* genutzt wird, bis der Anbieter das Problem geprüft hat. Diese menschliche Urteilskraft bleibt entscheidend.

Marktüberwachung heißt letztlich: **Vertraue keiner KI blind** – weder als Hersteller nach Auslieferung, noch als Nutzer im Betrieb. Die Systeme müssen im realen Einsatz beobachtet werden wie ein lebendes System. Unternehmen, die hier proaktiv agieren, können Vorfälle frühzeitig erkennen und adressieren, bevor Schaden entsteht (und bevor Behörden eingreifen müssen). Damit schützen sie nicht nur Nutzer, sondern auch sich selbst vor Haftung.

6. Menschliche Aufsicht und technische Robustheit sicherstellen

Was ist gefordert: Eine zentrale Anforderung des AI Act an Hochrisiko-Systeme ist die **menschliche Aufsicht** („human oversight"). Das bedeutet, dass KI-Systeme so konzipiert und genutzt werden müssen, dass Menschen ihre Funktionen nachvollziehen und bei Bedarf **eingreifen oder übersteuern** können [2]. Zugleich müssen KI-Systeme ein hohes Maß an **Robustheit, Genauigkeit und Cybersicherheit** aufweisen [28]. Zusammengenommen soll dies verhindern, dass KI unkontrolliert Schaden anrichtet.

Maßnahmen (für Entwickler und Betreiber):

- **„Human-in-the-loop"-Prinzip umsetzen:** Gestalten Sie die Nutzung Ihrer KI so, dass *kritische Entscheidungen* nicht ohne menschliche Freigabe erfolgen. Beispiele:
- In Personalentscheidungen: Eine KI filtert Bewerbungen vor, aber die finale Einladung oder Absage wird immer von einer HR-Person geprüft.
- In der Medizin: Die KI gibt eine Diagnose-Empfehlung, jedoch trifft der Arzt die endgültige Diagnose/Befundung und kann der KI auch widersprechen.
- In industrieller Steuerung: Die KI kann Warnungen oder Handlungsvorschläge geben, doch ein Mensch überwacht die Anlage und kann jederzeit manuell eingreifen (Not-Aus etc.).
  Wichtig ist, die **Rolle des Menschen klar zu definieren**: Welche Eingriffsmöglichkeiten bestehen? Ist der Mensch *informiert genug*, um sinnvoll zu übersteuern? (D.h. es muss ausreichend Transparenz oder Erklärbarkeit der KI-Entscheidung geben, damit der Mensch versteht, wann er einschreiten sollte.)

- **Aufsichtsprozesse und Training:** Unternehmen sollten entsprechende **SOPs (Standard Operation Procedures)** erstellen für den Betrieb mit KI:
- Wer überwacht die KI? (Zuständigkeit benennen, im Schichtbetrieb ggf. mehrere Personen schulen.)
- Welche Parameter oder Kennzahlen sollen Menschen im Blick haben? (Z. B. Konfidenzwerte der KI-Ausgaben; wenn unter X % Sicherheit, immer menschliche Prüfung.)
- Was ist im Eskalationsfall? (Z.B. wenn die KI ausfällt oder offensichtlich falsche Resultate liefert – wie schnell und durch wen wird das System abgeschaltet oder neu gestartet.)
  Schulen Sie die Mitarbeiter auf diese Prozesse. Ein*e* „Human-in-the-loop-Supervisor“ *braucht Kenntnisse sowohl über die fachliche Domäne als auch über die KI-Funktionsweise* [73] *. Stellen Sie sicher, dass Aufsichtspersonen wissen, wie die KI ungefähr funktioniert** und welche Eingriffe möglich sind [74] .
- **Erklärbarkeit sicherstellen:** Wo immer möglich, statten Sie Ihr KI-System mit **Erklärungsfunktionen** aus (sofern nicht inhärent erklärbar). Beispielsweise Feature Importance Scores, Entscheidungspfade oder wenigstens Hinweis auf Hauptfaktoren. Das hilft dem menschlichen Operator enorm bei der Überwachung. Wenn die KI ein „Black Box“-Modell ist, überlegen Sie, ob ein flankierendes erklärbares Modell oder Regeln eingebunden werden können, die zumindest grob veranschaulichen, warum die KI etwas vorschlägt.
- **Robustheitstests durchführen:** Testen Sie Ihre KI unter verschiedenen Bedingungen, um Robustheit sicherzustellen [28] :
- Variation der Eingabedaten (Noises, Extremwerte, andere Formate, bewusste *Stress-Tests*).
- Angriffsszenarien (falls relevant): z. B. bei Bilderkennung mal bewusst adversarial examples einspeisen, um zu sehen, wie leicht die KI auszutricksen ist. Für sicherheitskritische KI auch Penetration Tests in der Umgebung (IT-Sicherheit) durchführen.
- Performance-Monitoring: Überwachen Sie im Betrieb fortlaufend Genauigkeitsmetriken, sofern möglich. Falls die Leistung abdriftet (z. B. weil sich Daten verändert haben – Konzeptdrift), sollte eine Alarmierung erfolgen. Möglicherweise braucht es dann eine Neu-Trainierung oder Anpassung.
- **Fallback-Lösungen:** Halten Sie für den Fall von KI-Ausfällen *manuelle Verfahren* bereit. Beispiel: Wenn eine KI-gesteuerte Produktionsanlage ausfällt oder falsche Werte liefert, muss es einen manuellen Override geben, um die Produktion geordnet weiterzuführen. Im Kundenservice: wenn der Chatbot nicht weiter weiß, Übergabe an einen menschlichen Agenten. Diese Backups sollten nicht vergessen werden – KI dient zur Effizienz, aber kritische Prozesse sollten nicht völlig von ihr abhängen.
- **Cybersicherheit der KI:** Schützen Sie Ihre KI-Systeme vor unbefugtem Zugriff und Manipulation. Das umfasst:
- Zugangsbeschränkungen zu Modellen und Trainingsdaten (nicht jeder Entwickler darf live-Modellparameter ändern ohne Freigabe).
- Validierung der Eingaben, um Injection-Angriffe zu vermeiden (z. B. bei Text-KIs „Prompt Injection“ verhindern durch Sanitizing).
- Updates zeitnah einspielen, insbesondere sicherheitsrelevante Patches, auch für darunterliegende Libraries oder Frameworks.
- Protokollieren Sie sicherheitsrelevante Events (wer hat wann was am Modell gemacht). Diese Logs mindestens gemäß Gesetz aufbewahren (6 Monate oder länger, falls sinnvoll) [64] .
- **Regelmäßige Re-Evaluierung:** Menschliche Aufsicht und Technik müssen Hand in Hand gehen. Setzen Sie regelmäßige Meetings an, wo die „KI-Controller“ Feedback geben: Haben sie oft eingreifen müssen? Gab es Situationen, wo sie sich blind auf die KI verlassen haben? Daraus kann man lernen, entweder den Algorithmus zu verbessern oder die menschliche Rolle anzupassen.

Das Zusammenspiel von Mensch und KI ist letztlich ein **soziotechnisches System**. Die Verordnung fordert hier einen hohen Standard, um zu verhindern, dass KI-Fehler unbemerkt bleiben. Unternehmen

sollten nicht den Fehler machen, nach initialer Schulung dies zu vernachlässigen – kontinuierliche Aufmerksamkeit ist nötig. Gerade bei kreativen Einsätzen von KI sollte der Mensch als **kreativer Leiter** immer das letzte Wort haben, um sicherzustellen, dass die KI ein Hilfsmittel bleibt und nicht zum unkontrollierten Urheber wird. So können Risiken minimiert und die Stärken beider – menschliche Intuition und maschinelle Effizienz – optimal kombiniert werden.

Risiken und Chancen für Unternehmen

Die Umsetzung der KI-Verordnung birgt für Unternehmen sowohl Herausforderungen (**Risiken**) als auch strategische Vorteile (**Chancen**). Eine realistische Abwägung hilft, die richtige Einstellung gegenüber der Compliance-Aufgabe zu finden.

Risiken bei Nicht-Umsetzung oder falscher Umsetzung

- **Rechtliche und finanzielle Risiken:** Die offensichtlichste Gefahr ist, die Anforderungen zu ignorieren oder zu verfehlen. Ab 2026 drohen bei Verstößen empfindliche **Bußgelder** – je nach Schwere bis zu 30 Mio. € oder 6–7 % des weltweiten Jahresumsatzes [75] . Damit übersteigen die möglichen Strafen sogar die DSGVO-Bußgelder. Zusätzlich kann die Marktaufsicht **Produkte vom Markt nehmen** oder deren Einsatz untersagen, was zu direkten Umsatzeinbußen führt. Für kleine Firmen kann schon ein mittleres Bußgeld existenzbedrohend sein.
- **Haftungsrisiken:** Neben behördlichen Strafen drohen zivilrechtliche Konsequenzen. Die EU arbeitet parallel an einer KI-Haftungsrichtlinie, die es Geschädigten erleichtern soll, Unternehmen für KI-Schäden haftbar zu machen [76] [77] . Wenn etwa ein fehlerhaftes KI-System einen nachweisbaren Schaden anrichtet (Diskriminierungsfall, Gesundheitsschaden, Unfall), könnte das Unternehmen schadensersatzpflichtig werden. Ohne nachgewiesene Sorgfalt (Compliance) wird man sich kaum exkulpieren können.
- **Reputationsverlust:** In der Öffentlichkeit wächst das Bewusstsein für KI-Risiken. Ein Unternehmen, das durch einen KI-Skandal auffällt – sei es ein rassistischer Algorithmus im Recruiting [78] oder eine undurchsichtige KI, die Kunden verärgert – riskiert erheblichen **Imageschaden**. Vertrauen von Kunden und Geschäftspartnern kann verspielt werden, was langfristig schwerer wiegt als einmalige Strafen. Insbesondere in der Kreativbranche könnte schlechte PR (z. B. „Firma nutzt KI und verletzt Urheberrechte von Künstlern“) zu Boykotten führen.
- **Operative Risiken:** Die Umsetzung der Verordnung erfordert Ressourcen – Personal, Zeit, finanzielles Investment. Für kleinere Unternehmen kann dies kurzfristig belastend sein. Wer die Anforderungen unterschätzt, läuft Gefahr, **bis zum Stichtag 2026 nicht fertig** zu werden und dann hektisch (und fehleranfällig) Last-Minute-Lösungen zu improvisieren. Das kann den Geschäftsbetrieb stören. Ebenso könnte eine übertriebene Reaktion („KI vorsichtshalber komplett abschalten“) Innovationschancen verpassen lassen.
- **Innovationseinbußen:** Manche argumentieren, Regulierung könne Innovation hemmen. In der Tat besteht das Risiko, dass Unternehmen aus Angst vor Pflichten **auf KI verzichten**, obwohl sie nützlich wäre. Oder dass starre Compliance-Prozesse die agile Entwicklung verlangsamen. Gerade Start-ups mit knappen Mitteln könnten zögern, KI-Projekte zu starten. Langfristig wäre dies jedoch ein Nachteil im Wettbewerb – daher sollte man eher nach Wegen suchen, *trotz* Regulierung innovativ zu bleiben (z. B. durch Nutzung der KMU-Erleichterungen wie Sandboxes).

Chancen durch proaktive Umsetzung

- **Wettbewerbsvorteil durch Vertrauensbonus:** Unternehmen, die früh und sichtbar KI-Compliance umsetzen, können dies **marketingwirksam** nutzen. Ähnlich wie Bio-Siegel oder Datenschutz-Zertifikate kann ein „KI-konform nach EU-Recht“ zu einem Qualitätsmerkmal

werden. Kunden – ob Verbraucher oder Geschäftspartner – ziehen zunehmend Anbieter vor, denen sie in puncto **Verantwortung** vertrauen können. Ein sauber dokumentiertes, transparentes KI-Produkt wird z. B. im B2B-Vertrieb gegenüber einem Black-Box-Wettbewerber punkten (Stichwort: *Trustworthy AI* als Marke).

- **Prozessoptimierung und Professionalität:** Die erforderlichen Maßnahmen (Datenmanagement, Dokumentation, Risk Assessments) zwingen Unternehmen, ihre **internen Prozesse** zu verbessern. Dies hat oft positive Nebeneffekte: Bessere Datenqualität führt zu besseren Modellen; Dokumentation verhindert Wissensmonopole einzelner Entwickler und erleichtert Einarbeitung neuer Mitarbeiter; definierte Aufsichtsprozesse reduzieren operative Fehler. Kurz: Compliance kann Effizienz und Qualitätsmanagement stärken.
- **Innovation in neuen Bereichen:** Die Verordnung schafft **Rechtssicherheit** in vielen Fragen, was langfristig Innovation fördert. Beispielsweise wissen Hersteller nun, welcher Rahmen für Biometrie oder medizinische KI gilt – sie können gezielt Produkte entwickeln, die diese Hürden meistern, und damit Neuland betreten. In der Kreativbranche könnten klare Regeln zum KI-Einsatz neue Geschäftsmodelle hervorbringen (z. B. lizenzierte Datenpools für KI-Kunst, KI-Services für Künstler mit eingebauter Rechteverwaltung).
- **Zugang zu EU-Markt und Förderung:** Global agierende Unternehmen, die die EU-Regeln erfüllen, sind gut aufgestellt, da diese als **Vorbild für andere Regionen** dienen könnten. Wer jetzt investiert, hat später weniger Anpassungsaufwand, wenn etwa andere Länder ähnliche Gesetze einführen. Außerdem stellt die EU Förderprogramme und Netzwerke bereit (z. B. **AI-Sandkästen**, **Digital Innovation Hubs**), auf die konforme Unternehmen prioritären Zugriff haben [4] . KMU, die aktiv die angebotenen Unterstützungen nutzen, können mit geringerer Last neue KI-Lösungen pilotieren.
- **Mitarbeiter- und Talentgewinnung:** Gerade junge Fachkräfte in Tech und Kreativbereich achten auf die **ethische Dimension** ihres Arbeitgebers. Ein Unternehmen, das sich klar zu verantwortungsvoller KI bekennt und dies auch praktisch umsetzt, kann im War for Talent die Nase vorn haben. Intern fördert die Auseinandersetzung mit ethischen Fragen auch die Unternehmenskultur und kann zu mehr Sensibilität und Diversität beitragen (z. B. indem man interdisziplinäre Teams bildet für KI-Governance).
- **Reduziertes Risiko von KI-Pannen:** Last but not least – wer die Pflichten umsetzt, verringert real das Risiko, dass etwas schiefgeht. Viele Forderungen des Gesetzes (Tests, Oversight, Qualitätssicherung) sind ja *im eigenen Interesse* des Unternehmens: Sie minimieren teure Fehler, Rückrufe, Unfälle. Diese präventiven Maßnahmen sparen auf lange Sicht Kosten, die bei ungezügeltem Ausprobieren von KI entstehen könnten.

Spezifisch für Kreative: Auch hier gibt es Licht und Schatten. Risiken bestehen, dass z. B. strengere Regulierungen (oder auch Marktentwicklungen) bestimmte **KI-Tools in der Kunst unrentabel** machen oder den Zugang erschweren. Andererseits können Künstler, die sich jetzt als **„KI-kompetent und rechtsbewusst“** positionieren, neue Auftragspotenziale erschließen – etwa als Berater für KI-Einsatz in Medien, oder indem sie ihre eigene KI-gestützte Kunst als besonders ethisch deklarieren (z. B. „Trainiert nur auf gemeinfreien Daten“ etc.). Außerdem könnte mittel- bis langfristig ein **Fair-Use-Ausgleichssystem** kommen (Stichwort gesetzliche Lizenz gegen Vergütung [79]), was Kreativen ein neues Einkommen aus KI-Nutzung ihrer Werke verschafft. Wer bis dahin die Entwicklungen mitgeht, kann davon früh profitieren.

Fazit: Die EU-KI-Verordnung mag zunächst wie eine Compliance-Bürde wirken, doch ein bewusster Umgang kann sie zum **Strategietreiber** machen. Indem Unternehmen Risiken managen und transparent agieren, schaffen sie Vertrauen und setzen sich von weniger vorbereiteten Mitbewerbern ab. In einer Zeit, in der „vertrauenswürdige KI“ zum Schlagwort wird, sind diejenigen im Vorteil, die dieses Vertrauen aktiv aufbauen.

Handlungsempfehlungen

Abschließend folgen konkrete Empfehlungen als **Schritt-für-Schritt-Maßnahmen**, die Unternehmen jetzt ergreifen sollten, um die Umsetzung der KI-Verordnung effektiv anzugehen:

1. **Awareness schaffen & Zuständigkeit klären:** Informieren Sie die Geschäftsleitung und relevante Abteilungen über die kommenden KI-Regeln. Bestimmen Sie einen **KI-Compliance-Verantwortlichen** (oder ein Team), der das Thema koordiniert. Dieses Team sollte bereichsübergreifend arbeiten (IT/Entwicklung, Recht/Compliance, Fachabteilungen).
2. **KI-Inventur und Risikoklassifizierung durchführen:** Erstellen Sie eine Liste aller KI-basierten Systeme/Projekte im Unternehmen (inkl. Drittanbieter-Lösungen) und ordnen Sie diese gemäß den Kategorien *verboten – hochriskant – begrenzt – minimal* ein [2] [3]. Nutzen Sie dafür die im Businessplan beschriebenen Kriterien. Priorisieren Sie anschließend die hochriskanten und begrenzten Systeme für weitere Maßnahmen.
3. **Lückenanalyse und Maßnahmenplan:** Prüfen Sie für jedes identifizierte KI-System, welche konkreten Anforderungen die Verordnung stellt (z. B. braucht System A Transparenzhinweis, System B vollständige Doku und CE etc.). Erstellen Sie einen **Maßnahmenkatalog mit Verantwortlichkeiten und Zeitplan**. Beispiel: *„Für KI-System X: bis Q2/2025 Bias-Tests durchführen; bis Q4/2025 technische Dokumentation fertigstellen; Q1/2026 Konformitätserklärung unterschreiben."*
4. **Datenmanagement verbessern:** Setzen Sie umgehend Schritte zur **Daten-Governance** um. Säubern und dokumentieren Sie Ihre Datensätze, überprüfen Sie rechtliche Zulässigkeiten der Datenverarbeitung (DSGVO, Urheberrecht) und implementieren Sie nötige Verträge (z. B. Auftragsverarbeitung, Lizenzen für Datennutzung). Richten Sie Prozesse ein, um kontinuierlich die Datenqualität zu überwachen.
5. **Transparenz & UX-Updates:** Überarbeiten Sie UIs, Nutzerinformationen und Produktdokumentationen dahingehend, dass *wo nötig* KI offengelegt wird. Schulen Sie Marketing und Kundenservice, wie KI-Einsatz kommuniziert werden soll. Führen Sie ein, dass bei jeder neuen KI-Funktion gleich geprüft wird: **Braucht es einen Hinweis oder Label?** So wird Transparenz zur gewohnten Routine.
6. **Technische Dokumentation aufbauen:** Beginnen Sie frühzeitig, die **Dokumentationsstruktur** zu erstellen, vor allem für komplexe KI-Systeme. Auch wenn noch nicht alle Inhalte vorliegen – legen Sie Vorlagen an (Abschnitte laut Anhang IV der Verordnung) und füllen Sie nach und nach Informationen ein. Das verhindert Last-Minute-Stress. Nutzen Sie ggf. vorhandene Doku (aus QA, aus Entwicklungs-Dokumentation), um Dopplungen zu vermeiden.
7. **Standards und Tools nutzen:** Halten Sie Ausschau nach entstehenden **Branchenstandards** oder Normen für KI-Qualität und -Sicherheit. Diese könnten Ihnen viel Arbeit abnehmen (z. B. Standard-Testprotokolle, vordefinierte Bias-Kennzahlen). Verwenden Sie verfügbare **Open-Source-Tools** (für Fairness, Explainability, Security), um die technischen Anforderungen effizient zu erfüllen. Einige bekannte Tools: **Fairness 360**, **LIME/SHAP** für Erklärbarkeit, **Adversarial Robustness Toolbox** etc.
8. **Mitarbeiter schulen und Kultur fördern:** Organisieren Sie Trainings für Entwickler, Produktmanager und betroffene Fachkräfte zu den Kernthemen des AI Act. Machen Sie klar, dass **Verantwortung bei KI** Chefsache ist und alle angeht. Fördern Sie eine Kultur, in der ethische Aspekte von KI offen diskutiert werden. Mitarbeiter sollen sich trauen, potentielle Probleme anzusprechen (Whistleblower-Schutz bei KI-Vorfällen kann intern etabliert werden).
9. **Externe Beratung und Audit:** Ziehen Sie bei Unsicherheiten Fachexperten hinzu – etwa spezialisierte **Rechtsanwälte oder KI-Auditoren**. Ein *Pre-Audit* 2025 kann helfen, Schwachstellen aufzudecken, bevor die echten Prüfer kommen. Nutzen Sie Angebote wie **regulatorische Sandkästen**: In diesen von Behörden begleiteten Testräumen können Sie Ihre KI-Lösungen risikofrei erproben und Feedback der Aufsicht einholen [4].

10. **Kommunikation nach außen:** Informieren Sie auch Ihre Kunden und Partner über Ihren Ansatz zu KI-Compliance. Dies kann in Jahresberichten, auf der Website oder in Angebotsunterlagen passieren („Unser Unternehmen erfüllt bereits die Anforderungen der kommenden EU-KI-Verordnung…“). Transparenz schafft Vertrauen und differenziert Sie vom Wettbewerb.
11. **Kontinuierliches Monitoring bis zum Stichtag:** Verfolgen Sie die fortlaufenden Entwicklungen – etwa Ausführungsbestimmungen, nationale Gesetze zur Umsetzung, Leitfäden der Kommission. Passen Sie Ihren Umsetzungsplan an, falls es Änderungen gibt. Stellen Sie sicher, dass **bis Mitte 2026** alle notwendigen Schritte abgeschlossen sind. Nutzen Sie die Übergangszeit aber auch aus – etwa für Beta-Phasen in Sandkästen, um wirklich zum Stichtag ready zu sein.

Wenn Sie diese Empfehlungen befolgen, versetzen Sie Ihr Unternehmen in eine **proaktive Position**. Anstatt von der Regulierung überrascht zu werden, nutzen Sie die Zeit, um daraus einen **Wettbewerbsvorteil** zu formen. Wie bei Datenschutz nach Einführung der DSGVO wird sich zeigen: Firmen, die früh und ernsthaft investieren, ersparen sich spätere Schäden und genießen mehr Vertrauen. Im nächsten Abschnitt finden Sie noch einen Anhang mit einer kompakten Checkliste sowie nützlichen Tools und Links zur weiteren Vertiefung.

Anhang: Checkliste, Tools & Links

Checkliste zur KI-Compliance (Überblick):

- [ ] **KI-Systeme inventarisiert und klassifiziert** (inkl. Dokumentation der Risiko-Einstufung jedes Systems).
- [ ] **Verbotene KI-Praktiken ausgeschlossen** (keine Entwicklung/Nutzung von Social Scoring, manipulativer KI etc. gem. Art. 5 AI Act [32]).
- [ ] **Transparenz gewährleistet:** Nutzer werden bei KI-Interaktion informiert; KI-generierte Inhalte (insb. Deepfakes) sind klar gekennzeichnet [21] [22].
- [ ] **DSGVO-Konformität geprüft:** Rechtsgrundlagen für alle personenbezogenen Daten vorhanden; ggf. Datenschutz-Folgenabschätzung durchgeführt für KI-Verarbeitung sensibler Daten.
- [ ] **Datenqualität und -repräsentativität sichergestellt:** Trainings-/Testdaten bereinigt, Bias-Checks durchgeführt und dokumentiert; Datenquellen und Lizenzen erfasst [56].
- [ ] **Technische Dokumentation erstellt** (für Hochrisiko-Systeme gemäß Anhang IV AI Act: Systembeschreibung, Daten, Risiken, Testergebnisse, Anleitung etc. vollständig vorhanden).
- [ ] **Risikomanagement implementiert:** Risiken identifiziert, mitigiert und in Dokumentation nachverfolgt; laufender Prozess zur Risikoüberwachung etabliert.
- [ ] **Konformitätsbewertung durchgeführt:** Geprüft, ob Selbstbewertung oder externe Stelle nötig; alle erforderlichen Prüfungen bestanden; EU-Konformitätserklärung unterzeichnet [62].
- [ ] **CE-Kennzeichnung angebracht** (für Hochrisiko-KI-Systeme sichtbar am Produkt/Interface oder Unterlagen) [30]; Registrierung in EU-Datenbank erfolgt (falls vorgeschrieben).
- [ ] **Nutzerinformationen/Manual vorhanden:** Klare Anleitungen für Betrieb des KI-Systems an Kunden übergeben (inkl. Zweck, Leistungsdaten, Oversight-Hinweise, Wartung).
- [ ] **Menschliche Aufsicht gewährleistet:** Betriebsprozesse so gestaltet, dass menschliche Kontrolleingriffe möglich und vorgesehen sind; Personal geschult für Überwachung.
- [ ] **Genauigkeit/Robustheit nachgewiesen:** Validierungstests protokolliert; System zeigt geforderte Performance; Sicherheitsmaßnahmen gegen Angriffe umgesetzt.
- [ ] **Logging & Aufbewahrung:** KI-Systeme loggen automatisiert erforderliche Daten; Logs werden mind. 6 Monate sicher gespeichert (ggf. länger, gemäß branchenspez. Vorgaben) [64].
- [ ] **Post-Market Monitoring aktiv:** Feedback-Kanäle eingerichtet; Plan für regelmäßige Überprüfung der KI im Feld; Mechanismen zur Modellaktualisierung bei Drift.

- [ ] **Meldewesen etabliert:** Verantwortliche Person für Incident-Meldungen benannt; interne Schwellen definiert, was als meldepflichtiger Vorfall gilt; Meldeformular vorbereitet [71].
- [ ] **Zusammenarbeit mit Behörden:** Zuständige Aufsichtsbehörde bekannt; Prozesse für Auskunftsanfragen oder Audits definiert; ggf. Teilnahme an freiwilligen Audit-Programmen.
- [ ] **Mitarbeiter sensibilisiert:** Schulungen zu AI Act und ethischer KI durchgeführt; Verantwortlichkeiten klar; Unternehmenskultur unterstützt verantwortungsvollen KI-Einsatz.
- [ ] **Zukünftige Entwicklungen beobachtet:** Änderungen im Gesetzgebungsprozess (Delegierte Rechtsakte, Standards) im Blick; regelmäßiges Update-Meeting zur KI-Compliance eingeplant.

Nützliche Tools & Ressourcen:

- **Offizieller EU-Verordnungstext (Deutsch):** *Verordnung (EU) 2024/1689* – verfügbar im EUR-Lex Portal [47]. Enthält alle Artikel, Anhänge und Erwägungsgründe. Unverzichtbar für juristische Details.
- **EU KI-Act Explorer & Compliance-Checker:** Interaktive Website (artificialintelligenceact.eu) mit durchsuchbarem Gesetzestext und einem Werkzeug, das hilft einzuschätzen, ob ein System unter den AI Act fällt [80]. Praktisch für erste Einschätzungen und für KMU.
- **Leitfaden für KMU (EU AI Act):** Zusammenfassung der Bestimmungen mit Fokus auf kleine Unternehmen, inkl. Erläuterungen zu Erleichterungen und Tipps [81] [82]. Hilft KMU dabei, pragmatische Lösungen zu finden.
- **Branchenverbände & IHK:** Viele Verbände (Bitkom, VDMA, BDI etc.) erarbeiten derzeit branchenspezifische Leitfäden zur KI-Verordnung. Ebenso bieten Industrie- und Handelskammern Webinare und Checklisten an [83]. Es lohnt sich, dort Material zu beziehen, das auf die eigene Branche zugeschnitten ist.
- **ISO/IEC und CEN/CENELEC Standards:** Beobachten Sie die Entwicklung neuer KI-Normen. Z.B. wird an ISO 42001 (KI-Managementsystem) gearbeitet. Solche Standards können als Compliance-Grundlage dienen, sobald harmonisiert.
- **Technische Open-Source-Toolkits:**
- *AI Fairness 360 (IBM)* – Toolkit zur Prüfung und Mitigation von Bias in Daten und Modellen.
- *Adversarial Robustness Toolbox (ART by IBM)* – Bibliothek, um Modelle gegen Angriffe zu testen und robuster zu machen.
- *InterpretML oder LIME/SHAP* – Tools für erklärbare KI, um Entscheidungen für menschliche Aufsicht aufzuarbeiten.
- *Datasheets for Datasets* – Vorlage von Google/Partnership on AI für Datendokumentation (hilft bei Artikel 10-Compliance).
- **Regulatorische Sandkästen:** Informieren Sie sich bei Ihrer nationalen Behörde über AI-Sandboxes. In Deutschland z. B. plant die Regierung solche Testumgebungen. Teilnahme daran kann Ihnen praktische Einblicke und frühzeitige Kontaktnetze verschaffen.
- **Rechtlicher Rat & Literatur:** Nutzen Sie Whitepaper von Kanzleien (z. B. *DLA Piper's Key steps for organizations* [84], KPMG Law Beiträge [1] [10]) und Veröffentlichungen von Datenschützern (Datenschutzbehörden haben teils Q&As). Diese sekundären Quellen erklären komplexe Artikel oft mit Beispielen verständlich.
- **Kontaktstellen:** Die EU richtet ein *Europäisches Büro für KI* ein, zudem wird es nationale Kontaktstellen geben [85]. Dort können Unternehmen Fragen stellen und Hinweise erhalten. Sobald diese operativ sind, scheuen Sie nicht, dort Rat zu suchen.

Mit dieser Checkliste und den Werkzeugen sind Sie gut gerüstet, die Anforderungen der KI-Verordnung systematisch umzusetzen. Wichtig ist, **früh anzufangen und kontinuierlich dranzubleiben**. So wird aus einer gesetzlichen Pflicht ein Motor für bessere KI-Systeme und nachhaltigen Geschäftserfolg. **Viel Erfolg** bei der Umsetzung!

---

1 10 11 36 58 59 60 61 75 76 77 78 KI-Compliance: Wichtige rechtliche Aspekte im Überblick - KPMG-Law
https://kpmg-law.de/ki-compliance-wichtige-rechtliche-aspekte-im-ueberblick/

2 3 18 20 21 85 KI-Verordnung tritt in Kraft - Europäische Kommission
https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_de

4 5 81 82 Leitfaden für kleine Unternehmen zum AI Act | EU-Gesetz über künstliche Intelligenz
https://artificialintelligenceact.eu/de/small-businesses-guide-to-the-ai-act/

6 22 23 40 48 52 53 54 55 Leitfaden zur Kennzeichnung von KI-generierten Texten und Bildern | Mittelstand-Digital Zentrum Berlin
https://digitalzentrum-berlin.de/leitfaden-ki-generierte-inhalte-kennzeichnen

7 12 13 14 15 16 17 19 49 84 EU publishes its AI Act: Key steps for organizations | DLA Piper
https://www.dlapiper.com/en-us/insights/publications/ai-outlook/2024/eu-publishes-its-ai-act-key-considerations-for-organizations

8 9 39 Was das KI-Gesetz der EU für Kreative bringt - Kultur - SZ.de
https://www.sueddeutsche.de/kultur/anja-brauneck-kuenstler-urheberrecht-copyright-ai-act-eu-1.7251424

24 25 26 27 28 31 32 33 34 37 50 51 69 70 AI Act | Shaping Europe’s digital future
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

29 Was der AI Act für KI-Systeme bedeutet - LTO
https://www.lto.de/recht/hintergruende/h/ai-act-ki-verordnung-eu-sicherheit-risiko-teil-1

30 63 65 66 68 EU AI Act – Artikel 48: CE-Kennzeichnung
https://datenschutz-grundverordnung.eu/ai-act/artikel-48-ce-kennzeichnung/

35 47 79 EU Copyright Needs Reform to Spur Fair AI - CEPA
https://cepa.org/article/eu-copyright-needs-reform-to-spur-fair-ai/

38 42 43 44 45 Erwägungsgrund 105 | EU-Gesetz über künstliche Intelligenz
https://artificialintelligenceact.eu/de/recital/105/

41 46 Artikel 53: Verpflichtungen für Anbieter von KI-Modellen für allgemeine Zwecke | EU-Gesetz über künstliche Intelligenz
https://artificialintelligenceact.eu/de/article/53/

56 57 Artikel 10: Daten und Datenverwaltung | EU-Gesetz über künstliche Intelligenz
https://artificialintelligenceact.eu/de/article/10/

62 Artikel 47: EU-Konformitätserklärung | EU-Gesetz über künstliche ...
https://artificialintelligenceact.eu/de/article/47/

64 Artikel 26: Pflichten der Betreiber von KI-Systemen mit hohem Risiko
https://artificialintelligenceact.eu/de/article/26/

67 AI Act: Anforderungen an Einführer und Händler - datenschutz notizen
https://www.datenschutz-notizen.de/ai-act-anforderungen-an-einfuehrer-und-haendler-2449472/

71 Top 10 operational impacts of the EU AI Act – Post-market ... - IAPP
https://iapp.org/resources/article/top-impacts-eu-ai-act-post-market-monitoring-sharing-enforcement/

72 Article 73: Reporting of Serious Incidents | EU Artificial Intelligence Act
https://artificialintelligenceact.eu/article/73/

73 KI braucht Aufsicht: Die Rolle des Human in the Loop Supervisors ...
https://efarbeitsrecht.net/ki-braucht-aufsicht-die-rolle-des-human-in-the-loop-supervisors-hils/

74 Fachleute formulieren „KI-Grundregeln“ für menschliche Aufsicht
https://www.uni-saarland.de/aktuell/ki-grundregeln-menschliche-aufsicht-32580.html

80 EU AI Act Compliance Checker
https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/

83 AI Act: Regeln für Unternehmen beim Einsatz künstlicher Intelligenz
https://www.ihk-muenchen.de/de/Service/Digitalisierung/K%C3%BCnstliche-Intelligenz/AI-Act/