REGELN FÜR DIE KI-NUTZUNG

Praktische Umsetzung des EU-AI-ACTs

Die DSGVO als Kompass

Einleitung

Alle reden von Künstlicher Intelligenz und jeder der sie benutzt, lernt sie schnell zu schätzen. Längst laufen die Diskussionen in jedem Unternehmen und jeder sonstigen Institution, wie man Prozesse mit KI effizienter gestalten kann. Genauso geht aber auch die Angst um, dass man abgehängt wird, wenn man sich nicht möglichst umgehend mit KI beschäftigt.

Das Problem dabei: Die Informationen, über den rechtliche Rahmen für die KI-Nutzung, sind noch sehr unklar.

Seit August 2024 ist zwar der EU-AI-ACT in Kraft, aber der hat auf 144 Seiten zunächst einmal mehr Fragen aufgeworfen als beantwortet. Insbesondere verweist er darauf, dass die praktische Ausgestaltung der Verordnung in den Nationalstaaten in Form nationaler KI-Verordnungen stattfinden soll. Der grundsätzliche Rechtsrahmen ist also schon gesteckt, aber wie dieser praktisch umgesetzt wird, muss erst noch definiert werden. Aber genau das sind die Definitionen, die ein Unternehmen braucht, um rechtskonform arbeiten zu können.

Was der Gesetzgeber nicht berücksichtigt ist, dass alles, was im Rahmen der künstlichen Intelligenz passiert, sehr sehr schnell passiert. Die Systeme lernen und lernen, egal was der Gesetzgeber macht. Würde man also tatsächlich alle Regularien erst einmal für zwei Jahre aussetzen, wie es namhafte europäische Unternehmen gefordert haben, wären nachträgliche Regulierungen nur noch sehr schwer möglich.

Es besteht die Gefahr, dass viele Unternehmen und Institutionen, die KI jetzt schon einsetzen wollen, in der Übergangszeit bis zur nationalen Gesetzgebung oder sonstiger Aufschub-szenarien, KI in einer Form benutzen, wie es später möglicherweise nicht mehr erlaubt sein wird. Daten, deren Nutzung dann illegal ist, lassen sich aus den Systemen und Prozessen nur schwer wieder entfernen. Einen kleinen Vorgeschmack darauf erfahren gerade die Anbieter von KI-Modellen, die jetzt in der EU u. a. strengeren Regeln bezüglich der Urheberrechte bei Trainingsdaten unterliegen.

Aus dem Grunde sollte man einen Weg finden, wie man den rechtlichen Rahmen des EU-AI-ACTs schon so berücksichtigt, dass man zumindest bei den grundsätzlichen Rechtsauffassungen, die garantiert Kern der nationalen KI-Verordnungen sein werden, nicht abweicht.

Bei den Datenschutztagen vom Berufsverband der Datenschutzbeauftragten (BvD) am 27.05. – 28.05.2025 in Berlin wurde genau das Thema stark diskutiert. Teilnehmer war, neben der Bundesbeauftragten für den Datenschutz Frau Prof. Dr. Louisa Specht-Riemenschneider, auch zahlreiche Landesdatenschutzbeauftragte, also Mitglieder der Datenschutzkonferenz, die auch bei der Einführung der DSGVO federführend für die praktische Ausgestaltung der Gesetzesumsetzung waren. Alle Teilnehmer waren sich darin einig, dass die DSGVO der Kompass für den rechtlichen Rahmen des EU-AI-ACTs ist. Wie sollte es auch anders sein, denn sowohl in der DSGVO als auch im EU-AI-ACT steht natürlich der Schutz der Grundwerte und Grundfreiheiten der EU-Bürger bei der Datennutzung im Mittelpunkt.

In diesem Leitfaden habe ich, als Teilnehmer der Konferenz und nach intensiver Beschäftigung mit dem EU-AI-ACT, ausgearbeitet, wie die DSGVO und das Bundesdatenschutzgesetz (BDSG) Leitplanken für eine sichere Nutzung von künstlicher Intelligenz setzen können. Außerdem habe ich die wichtigsten Begriffe, Definitionen und Ansätze des EU-AI-ACTs zusammengefasst, damit ein gemeinsames Verständnis geschaffen werden kann.

Was ist Künstliche Intelligenz?

Zunächst einmal muss man wissen, dass nicht alles KI ist, was als KI verkauft wird. Künstliche Intelligenz ist längst ein Marketing-Hype geworden, mit dem sich einfache Systeme teuer verkaufen lassen.

Der EU-AI-ACT greift aber nur bei echter Künstlicher Intelligenz, die in der Verordnung auch genau definiert ist. Hier eine Beschreibung mit eigenen Worten und Beispielen:

Künstliche Intelligenz lässt sich als Simulation menschenähnlicher kognitiver Prozesse durch Computerprogramme bezeichnen. Anders als herkömmliche Algorithmen basierte IT-Systeme, die für sehr spezifische Aufgaben programmiert werden und nur auf festgelegten Regeln basieren, kann KI aus Daten lernen und ihre Leistung im Laufe der Zeit verbessern. Kurz gesagt:

- KI ist flexibel, lernfähig und kann komplexe, nicht vorhersehbare Probleme lösen.
- Algorithmen basierte Systeme sind starr, regelbasiert und lösen klar definierte Aufgaben.

Beispiel für KI: Ein medizinisches Diagnosesystem, das Röntgenbilder analysiert und auf Basis tausender gelernter Fälle selbstständig erkennt, ob ein Tumor vorliegt. Es lernt kontinuierlich dazu, je mehr Daten es verarbeitet.

Beispiel für ein Algorithmen basiertes System: Ein Krankenhausverwaltungssystem, das Patienten nach festen Kriterien (z. B. Nachname, Geburtsdatum etc.) sortiert und Termine automatisch vergibt. Es führt exakt die programmierten Schritte aus, ohne sich an neue Muster oder Anforderungen anzupassen.

Unterscheidung KI-Systeme und KI-Modelle

Künstliche Intelligenz wird in KI-Modelle und KI-Systeme unterschieden.

Ein **KI-Modell** ist der mathematische oder algorithmische Kern einer künstlichen Intelligenz. Es handelt sich um eine trainierte Struktur – etwa ein neuronales Netz oder ein Entscheidungsbaum, die auf Basis von Daten Muster erkennt, Vorhersagen trifft oder Entscheidungen vorbereitet. Das KI-Modell selbst ist jedoch nicht direkt nutzbar, sondern benötigt eine Umgebung, in der es eingebettet wird.

Ein **KI-System** hingegen ist die vollständige Anwendung, die ein oder mehrere KI-Modelle integriert und weitere Komponenten wie Datenverarbeitung, Benutzeroberflächen, Schnittstellen und Steuerungslogik kombiniert. Es ist das, was tatsächlich in der Praxis eingesetzt wird – etwa in einem Krankenhaus, einem Chatbot oder einer Verkehrssteuerung.

Das KI-Modell ist wie der Motor eines Autos – leistungsstark, aber ohne Karosserie, Steuerung und Räder nicht fahrbereit. Das KI-System ist das komplette Fahrzeug, das den Motor nutzt, um Menschen sicher von A nach B zu bringen.

Rollen im KI-Umfeld

Bei der Frage, welche Regularien für wen gelten, ist es entscheidend, welche Rolle man bei der KI-Nutzung einnimmt. Der EU-AI-ACT definiert mehrere Rollen, die jeweils unterschiedliche Pflichten und Verantwortlichkeiten mit sich bringen. Hier sind die wichtigsten Rollen, die man einnehmen kann:

ROLLE	BESCHREIBUNG	BEISPIELHAFTE PFLICHTEN
Betreiber	Nutzt ein KI-System für eigene Zwecke, z. B. zur Prozessoptimierung oder Kundenservice	Sicherstellung der rechtskonformen Nutzung, Risikoabschätzung
Anbieter	Entwickelt oder vertreibt ein KI-System unter eigenem Namen	Konformitätsbewertung, technische Dokumentation, Transparenz
Einführer	Bringt ein KI-System aus einem Drittland in die EU	Prüfung auf Einhaltung der EU-Vorgaben, Dokumentationspflichten
Bevollmächtigter	Vertritt einen Anbieter außerhalb der EU und übernimmt dessen Pflichten	Kommunikation mit Behörden, Sicherstellung der Konformität
Händler	Vertreibt KI-Systeme, ohne sie selbst zu entwickeln	Weitergabe von Informationen, Rückverfolgbarkeit

Der EU-AI-ACT verfolgt einen risikobasierten Ansatz

KI-Systeme werden im EU-AI-ACT danach unterschieden, mit welchem Risiko für die Gesellschaft sie behaftet sind. Entsprechend dieser Einteilung ergibt sich auch der Regelungsbedarf, dem die Unternehmen, die KI einsetzen, unterliegen. Im EU-AI-ACT gibt es vier Risikokategorien:

RISIKOSTUFE	BEISPIEL	REGELUNG
Unannehmbares Risiko	Social Scoring, manipulative Verhaltenssteuerung	Diese Systeme sind in der EU **verboten**
Hohes Risiko	KI in der Medizin, Justiz, Bildung, kritischer Infrastruktur	**Strenge Anforderungen:** Konformitätsbewertungen, Dokumentation, Transparenz
Begrenztes Risiko	Chatbots, KI-generierte Inhalte	**Transparenzpflichten:** z. B. Hinweis auf KI-Interaktion
Minimales Risiko	KI in Videospielen, intelligente Spamfilter	**Keine spezifischen Vorgaben**

Mit den unannehmbaren Risikosystemen muss man sich nicht länger beschäftigen. Da ist es ganz einfach – sie sind **VERBOTEN!**

Bei Systemen mit minimalem Risiko neigt man dazu, sie einfach einzusetzen, ohne sich Gedanken zu machen. ABER VORSICHT: Die Entscheidungsfindung, ob es sich wirklich um ein System mit minimalem Risiko handelt, muss natürlich richtig und nachvollziehbar sein. Unter Umständen ist also auch hierbei eine beratende Unterstützung nötig, denn eine Fehlentscheidung stellt ein Verstoß gegen den EU-AI-ACT dar.

Am wichtigsten sind allerdings KI-Systeme mit begrenztem und hohem Risiko, denn dafür gibt es auf jeden Fall Regelungen, die eingehalten werden müssen.

Hochrisiko-KI-Systeme

Die Hochrisiko-KI-Systeme sind in den Anhängen I, II und III des EU-AI-ACTs genauer beschrieben. Kurz auf den Punkt gebracht, geht es im **Anhang I** um die Harmonisierung mit anderen Vorschriften, die bestimmte Bereiche bereits vorher reguliert haben. Das gilt z. B. für den Einsatz von Kraftfahrzeugen, Eisenbahnen, Aufzüge, Funkanlagen etc. Wer Leistungen in diesen Bereichen anbietet, wird wissen, dass es bereits besondere Regularien gibt. Diese werden in Zukunft um die KI-Themen erweitert.

In **Anhang II** geht es in erster Linie um die Strafverfolgung und die Justiz. Also kein Thema für die private Wirtschaft.

Wichtig für jedes Unternehmen ist allerdings der **Anhang III**, denn dort werden auch z. B. Punkte wie:

- Biometrische Identifizierung und Kategorisierung von natürlichen Personen
- Beschäftigung, Verwaltung der Arbeitnehmer und Zugang zur Selbstständigkeit

aufgeführt. Damit ist man unter anderem im Bereich von **KI in HR-Systemen**. Hier gilt es also vorsichtig zu sein, welche Funktionen bei solchen Systemen zum Einsatz kommen.

Kurz gesagt: Kommt man in den Bereich der Hochrisiko-KI-Systemen muss man auf jeden Fall eine Konformitätsbewertung mit Folge- und Risikoabschätzung machen. In vielen Fällen wird man auch eine behördliche Genehmigung brauchen. Inwieweit die behördliche Genehmigung auch für die HR-Systeme zutrifft, wird sich erst herausstellen, wenn der EU-AI-ACT in nationales Recht umgesetzt ist.

KI-Systeme mit begrenztem Risiko

Beim Einsatz von KI-System mit begrenztem Risiko benötigt man natürlich auch wieder einen nachvollziehbaren Entscheidungsprozess, der zu der richtigen Risikoeinschätzung geführt hat.

Aus dem Grund schreibt der EU-AI-ACT sowohl bei Hochrisiko-KI-Systemen, als auch bei KI-Systemen mit begrenztem Risiko, **KI-Kompetenz** im Unternehmen vor. Gemäß Artikel 4 EU-AI-ACT müssen Unternehmen sicherstellen, dass alle Personen, die mit KI-Systemen arbeiten – ob

intern oder extern – über ein „ausreichendes Maß an KI-Kompetenz“ verfügen. Das betrifft Anbieter, **Betreiber** und **Nutzer** von KI-Systemen.

Und das gilt eben auch bei begrenztem Risiko, z. B. bei Chatbots oder Textgeneratoren.

Der KI-Beauftragte

Im EU-AI-ACT kommt auch der KI-Beauftragte zur Sprache. Die Verordnung schreibt aber keine explizite Person dafür vor, wie zum Beispiel in der DSGVO der Datenschutzbeauftragte. Ob ein KI-Beauftragter in der deutschen Gesetzesumsetzung vorgeschrieben wird, bleibt abzuwarten. Allerdings wird ganz sicher eine Rolle definiert werden, die verantwortlich ist für die:

- Entwicklung von internen KI-Richtlinien (z. B. „*Acceptable Use Policy*“)
- Aufbau und Erhalt der KI-Kompetenz
- Beratung und Dokumentation der Entscheidungsprozesse
- Folge- und Risikoabschätzungen

etc.

Es fällt auf, dass die Aufgaben dieser Rolle sehr den Aufgaben der Rolle des Datenschutzbeauftragten ähnlich sind.

Bei der Datenschutzkonferenz des Bundesverbandes der Datenschutzbeauftragten (BvD) am 27. – 28.05.2025 in Berlin, bei dem der Verfasser dieses Papieres anwesend war, wurde offen diskutiert, ob der Datenschutzbeauftragte die Rolle des KI-Beauftragten übernehmen könnte. Von Seiten der Bundesbeauftragten für den Datenschutz und auch von den anwesenden Landesdatenschutzbeauftragten wurde dieser Ansatz ausdrücklich begrüßt. Jedenfalls wollten sich die Genannten dafür einsetzen, dass das so in der nationalen Gesetzgebung berücksichtigt wird. Ob das tatsächlich so passiert, ist natürlich nicht sicher.

Derzeit ist auch noch nicht sicher, wie genau die Qualifikationen der KI-Beauftragten-Rolle spezifiziert werden. Es werden zwar schon viele teure Zertifizierungskurs angeboten, aber ob die die richtigen Inhalte vermitteln, weiß aktuell keiner.

Warum es dennoch kein Fehler ist, in dieser Übergangszeit, vor dem KI-Einsatz mit dem Datenschutzbeauftragten zu sprechen, zeigen die nächsten Kapitel.

Rechtsrahmen - die DSGVO als Kompass

Um den Rechtsrahmen abschätzen zu können, in der sich die nationale KI-Gesetzgebung bewegen wird, beschreibt der EU-AI-ACT zwei grundsätzliche Überlegungen:

- Überlegungen zum ethnischen Rahmen der KI-Nutzung
- Überlegungen zum Datenschutz bei der KI-Nutzung

Überlegungen zum ethnischen Rahmen der KI-Nutzung

Bei der ethischen Bewertung von KI-Produkten ist eine wertorientierte Technologiegestaltung entscheidend. Die Werte, die hierbei berücksichtigt werden sollten, hängen vom Einsatzkontext ab.

Es existieren verschiedene Ansätze für die ethische Bewertung von KI, wie beispielsweise die Ethik-Leitlinien der EU-Kommission oder die Stellungnahme des Deutschen Ethikrats. Jedenfalls sind das ähnliche Ansätze, wie sie bereits bei der Entwicklung der DSGVO zum Einsatz kamen.

So wird z. B. als wichtiger Wert bei der Entwicklung und dem Betrieb von KI die Transparenz beschrieben. Hierbei sollten die Funktionen und Verarbeitungsmethoden der KI-Systeme mindestens für die relevanten Zielgruppen angemessen offen und verständlich sein, um das sogenannte Blackbox-Phänomen zu vermeiden.

Bei der Fairness von KI-Anwendungen sollte bereits bei der Entwicklung darauf geachtet werden, dass Verzerrungen in den Ergebnissen und Diskriminierung vermieden werden. Stattdessen sollten KI-Anwendungen Vielfalt und Chancengleichheit fördern.

Insgesamt sollten ethische Kriterien in der KI-Entwicklung und im KI-Betrieb zu einem ganzheitlichen Risikomanagement beitragen, zentrale demokratische Werte wahren und deren Operationalisierung nachvollziehbar gestalten.

Überlegungen zum Datenschutz im Rahmen der KI-Nutzung

Die regulatorischen Ziele der Europäischen Union im Bereich der Datenwirtschaft und der künstlichen Intelligenz haben die klare Vision, den Schutz der Bürgerrechte, die Förderung von Innovation und die Schaffung eines fairen und transparenten digitalen Binnenmarktes in Einklang zu bringen.

Ein zentraler Bestandteil bleibt die DSGVO, die die Verarbeitung personenbezogener Daten reguliert und Standards für den Schutz der Privatsphäre setzt. Der Anwendungsbereich der DSGVO erstreckt sich auf personenbezogene Daten, die in KI-Systemen genutzt werden. Ob personenbezogene Daten zum Einsatz kommen, ist wiederum das Ergebnis eines nachvollziehbaren, dokumentieren Prüfungsprozesses. Gemäß Art. 1 DSGVO ist eine Person identifizierbar, die direkt oder indirekt, z. B. mittels Zuordnung zu einem Namen, einer Kennnummer, Standortdaten oder zu einem oder mehreren besonderen Merkmalen, identifiziert werden kann.

In dem Rahmen gelten auch bei der KI-Nutzung die einschlägigen Bestimmungen aus der DSGVO z. B. die Einhaltung der Datenschutzgrundsätze nach Artikel 5 DSGVO:

- Rechtmäßigkeit, Art. 5 (1) a) Alt. 1 DGGVO
- Treu und Glauben, Art. 5 (1) a) Alt. 2 DSGVO
- Transparenz, Art. 5 (1) a) Alt. 3 DSGVO
- Zweckbindung, Art. 5 (1) b) DSGVO
- Datenminimierung, Art. 5 (1) c) DSGVO
- Richtigkeit, Art. 5 (1) d) DSGVO
- Rechenschaftspflicht, Art. 5 (2) DSGVO

Für das Trainieren von künstlicher Intelligenz ist das Vorliegen einer Rechtsgrundlage ein wesentlicher Schritt für eine rechtskonforme Verarbeitung personenbezogener Daten. Als Rechtsgrundlage kommen grundsätzlich die Einwilligung (Art. 6 (1) a) DSGVO, Art. 9 (2) a) DSGVO), die Verarbeitung im Rahmen der Vertragserfüllung (Art. 6 (1) b) DSGVO) sowie die Verarbeitung zur Wahrung berechtigter Interessen (Art. 6 (1) f) DSGVO) für Unternehmen im nicht öffentlichen Bereich in Betracht.

Weitere DSGVO-Artikel, die bei der KI-Nutzung beachtet werden müssen, sind:

- Artikel 9 DSGVO: Verarbeitung besonderer Kategorien personenbezogener Daten
- Transparenz und Informationspflichten (z.B. Artikel 13 und 14)
- Artikel 12 ff. DSGVO: Umsetzung von Betroffenenrechten (Insbesondere: Sicherstellung der Betroffenenrechte im „Data Lake“)
- Artikel 24 ff. DSGVO: Datenschutzrechtliche Verantwortlichkeit (alleinige Verantwortung, gemeinsame Verantwortung, Auftragsverarbeitung)
- Artikel 25 ff. DSGVO: Privacy by Design/Privacy by Default und Einsatz von geeigneten technischen und organisatorischen Maßnahmen
- Artikel 30 DSGVO: Aufnahme der Verarbeitung in das Verzeichnis von Verarbeitungstätigkeiten
- Artikel 33, 34 DSGVO: Prozess Datenschutzvorfall
- Artikel 35 DSGVO: Durchführung einer Datenschutzfolgeabschätzung einschl. Risikoabwägungen.

Außerdem müssen KI-Systeme Bestandteil des Berechtigungs- und des Löschkonzeptes sein.

Es ist also deutlich erkennbar, dass die DSGVO der Kompass für die Datenschutzregelungen im EU-AI-ACT ist und somit auch in der nationalen Gesetzgebung sein wird.

Fazit

Der vorliegende Leitfaden bietet eine praxisnahe Orientierung für den rechtskonformen Einsatz von Künstlicher Intelligenz im Unternehmenskontext. Er zeigt, dass der EU-AI-ACT zwar einen verbindlichen Rahmen vorgibt, dessen konkrete Umsetzung jedoch maßgeblich von der nationalen Gesetzgebung abhängt. In dieser Übergangsphase kommt der DSGVO eine zentrale Rolle zu – sie dient als rechtlicher Kompass und bietet bereits heute klare Vorgaben für den Umgang mit personenbezogenen Daten in KI-Systemen.

Besonders hervorzuheben ist der risikobasierte Ansatz der KI-Verordnung, der Unternehmen dazu verpflichtet, ihre Systeme sorgfältig zu klassifizieren und entsprechende Maßnahmen zu ergreifen. Die Einführung einer verantwortlichen Rolle – etwa eines KI-Beauftragten – erscheint nicht nur sinnvoll, sondern könnte auch gesetzlich verankert werden.

Wer KI bereits heute einsetzen möchte, sollte nicht auf die endgültige nationale Umsetzung warten, sondern proaktiv handeln: durch Risikoanalysen, Kompetenzaufbau und die Einbindung datenschutzrechtlicher Expertise. Nur so lässt sich sicherstellen, dass Innovation und Rechtssicherheit Hand in Hand gehen.

(*Dieses Fazit wurde durch eine KI verfasst*)