

DATENSCHUTZ

KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Alles Neu: Informationsfreiheit und KI

**IFG und die Herausforderungen
des Datenschutzes**

Interview mit Markus Hametner, Forum Informationsfreiheit

IFG: ein Überblick

Rainer Knyrim und Stephan Varga

Einsatz von KI als neuartige Datenverarbeitung?

Moritz W. Rothmund-Burgwall

Checkliste AI Act

Hans-Jürgen Pollirer

Inhaltskontrolle von Datenschutztexten

Lena Maria Urban und Stephanie Briegl

DSA: Neue Regelungen für Online-Werbung

Martin Baumann und Felix Mikolasch

Rechtsprechung: Dash Cams im Einzelfall zulässig

Viktoria Haidinger und Michael Löffler



Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste AI Act

Anwendungsbereich; risikobasierter Ansatz; Dokumentation; Qualitätsmanagementsystem; Transparenzpflichten. Kern des AI Act ist ein risikobasierter Ansatz, wobei das Risikopotential anhand von vier Risikofeldern qualifiziert wird. Die Checkliste dient als erste Information für die verschiedenen Akteure, die von den Bestimmungen des AI Act betroffen sind.

Einleitung

Bereits in der Dako 2023/44 ist eine „Checkliste Künstliche Intelligenz und Datenschutz“ erschienen. Zu diesem Zeitpunkt

wurde gerade am 18. 7. 2023 im zweiten Triolog eine Einigung zwischen EP und Rat in Bezug auf die Vorschriften für Anbieter von Hochrisiko-KI-Systemen und zu den

Bestimmungen zur Einhaltung dieser Vorschriften in einem Konformitätsbewertungsverfahren sowie zu technischen Standards erreicht. Die **Zeitleiste der Entwick-**

lungen des AI Act bei Verlassen dieses Beitrags stellt sich wie folgt dar:

- Nach weiteren Trilog-Sitzungen am 2., 3. und 24. 10. konnte in der fünften Trilog-Sitzung am 9. 12. 2023 endlich eine Einigung zwischen Rat und EP erzielt werden.
- Am 2. 2. 2024 bewilligte der Rat einstimmig den Gesetzesentwurf über den EU AI Act.
- Am 13. 2. 2024 stimmte der Ausschuss für Binnenmarkt und bürgerliche Freiheiten mit 71:8 Stimmen – bei 7 Stimmenthaltungen – für die Annahme des Ergebnisses der Verhandlungen mit den MS über den AI Act. Damit haben die 27 MS den AI Act einstimmig gebilligt.
- Am 13. 3. 2024 stimmte auch das EP dem Gesetzesentwurf zu.¹
- Anschließend muss der AI Act noch von Rechts- und Sprachsachverständigen geprüft werden und die Annahme im Rahmen des Berichtungsverfahrens erfolgen.
- Der AI Act tritt 20 Tage nach seiner Veröffentlichung in Kraft und gilt primär ab dem 24. Monat für Hochrisiko-KI-Systeme sowie für die Transparenzvorschriften und Sandboxes, jedoch tritt **schrittweise** für folgende Bestimmungen **in Kraft** (Art 113):
 - 6 Monate: Systeme mit inakzeptablem Risiko werden verboten;
 - 12 Monate: die Vorschriften für KI mit allgemeinem Verwendungszweck und Basismodelle gelten;
 - 36 Monate: die Regeln für Hochrisiko-IT-Systeme gem Anh III gelten.

Der AI Act ist der erste Rechtsrahmen der EU für KI und soll nach Ansicht der EK Europa in die Lage versetzen, weltweit eine führende Rolle bei der Festlegung von globalen Standards zu spielen. Er ist Teil eines umfassenden Pakets politischer Maßnahmen zur Unterstützung und Entwicklung vertrauenswürdiger KI, zu dem auch das KI-Innovationspaket² und der koordinierte KI-Plan³ gehören sowie die AI Liability Directive,⁴ die Vorschriften zu außervertraglichen Haftungsfragen iZM KI-Systemen regeln soll. Des Weiteren ist auch eine Überarbeitung der sektoralen Sicherheitsvorschriften (zB Produktsicherheit) geplant.

Der AI Act ist sehr umfangreich, er enthält 180 ErwGr, 113 Artikel und 13 Anhänge. Er fordert, dass KI-Anwendungen nicht nur effizient, sondern auch sicher, transparent, ethisch korrekt und grundrechtskonform gestaltet sein müssen.

Art 3 Z 1 definiert ein KI-System wie folgt, wobei aufgrund der zum Zeitpunkt der Erstellung des Beitrags noch nicht vorliegenden juristisch und sprachlich geprüften Fassung des AI Act auf die englische Fassung zurückgegriffen wird:

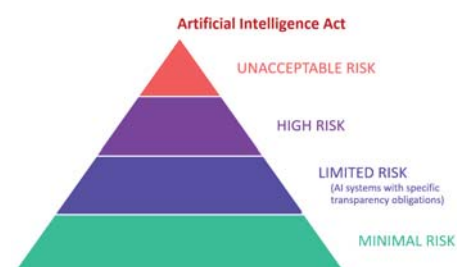
„AI system‘ means a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments; [...]“

Die **Nichtbeachtung** der Bestimmungen des AI Act ist mit hohen **Bußgeldern** verbunden, und zwar:

- Bis zu 35 Mio Euro bzw 7% des weltweiten Jahresumsatzes (davon abhängig, welcher Wert höher ist) bei Missachtung der in Art 5 genannten KI-Praktiken in Bezug auf verbotene KI-Systeme oder die Nichteinhaltung der Anforderungen an Daten.
- Bis zu 15 Mio Euro bzw 3% des weltweiten Jahresumsatzes (davon abhängig, welcher Wert höher ist) bei Verstößen gegen geltende Bestimmungen für Anbieter (Art 16), Bevollmächtigte (Art 22) sowie Einführer (Art 23), Händler (Art 24), Betreiber (Art 26), notifizierte Stellen (Art 31, 33 Abs 1, 3 und 4, Art 34), Transparenzpflichten für Anbieter und Nutzer (Art 50).
- Bis zu 7,5 Mio Euro bzw 1% des weltweiten Jahresumsatzes (davon abhängig, welcher Wert höher ist) bei Falschaussagen bzw unvollständigen oder irreführenden Informationen an notifizierte Stellen oder zuständige Behörden.

Im Falle von KMUs gilt aber der jeweils niedrigere Betrag.

Kern des AI Act ist ein **risikobasierter Ansatz**, wobei das Risikopotential anhand der nachstehenden vier Risikofelder qualifiziert wird:



Quelle: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

- **Inakzeptables Risiko** (Unacceptable Risk): Betrifft KI-Systeme, die eine eindeutige Bedrohung für die Sicherheit, die Lebensgrundlage und die Menschenrechte darstellen. Darunter fallen zB KI-Systeme wie Social Scoring, die Menschen sozial bewerten, Systeme zur biometrischen Klassifizierung in Bezug auf die in den Art 9 und 10 DSGVO als besonders schützenswert angeführten Daten uÄ (Art 5).

- **Hohes Risiko** (High Risk): Diese Gruppe stellt den bedeutendsten Anwendungsbereich des AI Act dar und ist von den meisten Bestimmungen betroffen. Sie enthält den Einsatz von KI-Systemen in sensiblen Lebensbereichen und ist aufgrund ihrer Risikoneigung besonders stark reglementiert. In diese Gruppe fallen KI-Systeme in kritischen Infrastrukturen (Verkehr, Wasser, Gas-, Wärme- und Stromversorgung), im Bildungs- und Berufswesen (zB Bewerberauswahl), Strafverfolgung, private und öffentliche Dienstleister (zB Bonitätsprüfung) uÄ (Art 6 bis 49, Anh III).

- **Begrenztes Risiko** (Limited Risk): Umfasst KI-Systeme, von denen nur ein begrenztes Risiko ausgeht, wie zB Chatbots. Für diese Gruppe gelten spezifische Transparenzpflichten (Art 51, Anh XIII).

- **Minimales Risiko** (Minimal Risk): Der AI Act erlaubt die freie Nutzung von KI-Systemen mit minimalem Risiko. Diese Gruppe betrifft die überwiegende Mehrheit der derzeit in der EU eingesetzten KI-Systeme, wie zB Spamfilter oder KI-fähige Videospiele.

In der politischen Diskussion war insb die Einbeziehung von „**General Purpose AI Models**“ (GPAI) besonders umstritten. Unter diesen „KI-Systemen mit allgemeinem Verwendungszweck“ versteht man KI-Systeme, die allgemeine Funktionen wie Bild- und Spracherkennung, Videogenerierung, Mustererkennung, Beantwortung von Fragen sowie Übersetzungen usw ausführen. Darunter fallen **Large Language Models** (LLM) und andere **generative AI-Tools** wie ChatGPT, Google Gemini, Bing AI. Entsprechend der im AI Act festgelegten Logik werden die GPAI-Modelle in die dritte Risikostufe eingeordnet. Dabei werden **zwei Gruppen unterschieden**,

¹ www.europarl.europa.eu/doceo/document/TA-9-2024-0138_DE.html/ ² <https://kurzelinks.de/0yjn> ³ <https://kurzelinks.de/wbqa> ⁴ <https://kurzelinks.de/faii>

die checkliste

und zwar GPAI „mit allgemeinem Zweck“ und GPAI „mit erheblichen Auswirkungen“, wobei diese Differenzierung nicht auf die Anwendung selbst, sondern auf die Rechenleistung und Reichweite des zugrundeliegenden Basismodells Bezug nimmt. Die **Rechenleistung** wird in Gleitkommaoperationen pro Sekunde (Floating Point Operations Per Second, FLOP) gemessen. Art 51 Z 2 legt den Schwellenwert für GPAI mit erheblichen Auswirkungen mit 10²⁵ FLOP fest.

Der AI Act sieht eine Verwaltungsstruktur mit mehreren zentralen **Regulierungsbehörden** vor, die jeweils unterschiedliche Aufgaben in Bezug auf die Umsetzung und Durchsetzung des AI Act wahrnehmen sollen. Im Einzelnen sind dies:

Auf EU-Ebene

- Einrichtung eines AI Office, das bereits am 24. 1. 2024 gegründet wurde und die Umsetzung und Durchsetzung des AI Act gewährleisten soll (Art 64).
- Des Weiteren wird ein „Europäischer Ausschuss für Künstliche Intelligenz“ eingerichtet, der sowohl die EK als auch die MS unterstützen soll, um eine ein-

heitliche und wirksame Anwendung des AI Act zu erleichtern (Art 65).

- Weiters soll ein Beratungsforum aus unabhängigen Experten den Ausschuss und die EK beraten (Art 67).
- Schlussendlich soll ein wissenschaftliches Gremium unabhängiger Sachverständiger eingerichtet werden, das die Durchsetzungstätigkeiten im Rahmen des AI Act unterstützen soll (Art 68).

Auf nationaler Ebene

- Jeder MS muss mindestens eine notifizierende Behörde einrichten, die insb KMU einschließlich Start-up-Unternehmen bei der Durchführung des AI Act zur Seite stehen und die ordnungsgemäße und rechtzeitige Durchführung von Konformitätsbewertungen sicherstellen soll (Art 70). Vorerst wurde die **KI-Servicestelle** mit Beschluss des Nationalrats vom 21. 1. 2024 in der Rundfunk und Telekom Regulierungs-GmbH (RTR) eingerichtet, die in einem weiteren Ausbaus Schritt in eine KI-Behörde übergeht.
- Jeder MS muss darüber hinaus auch mindestens eine **Marktüberwachungsbehörde** einrichten, die zur Durchfüh-

rung externer Konformitätsbewertungen berechtigt ist (Art 70).

Vom AI Act sind unterschiedliche Akteure betroffen (Art 2):

- Anbieter (A)
- Betreiber (B)
- Einführer und Händler (C)
- Produkthersteller (D)
- Bevollmächtigte von Anbietern (E)
- betroffene Personen (F)

Der Sitz in einem **Drittstaat** entbindet Anbieter, Betreiber und Bevollmächtigte nicht von den im AI Act normierten Pflichten, wenn das KI-System für die EU bestimmt ist oder das vom KI-System hervorgebrachte Ergebnis in der EU verwendet wird.

Die Checkliste dient als erste Information für die verschiedenen Akteure, die von den Bestimmungen des AI Act betroffen sind. Da die Annahme, dass der AI Act am 10. 4. 2024 nach Abschluss des Berichtigungsverfahrens endgültig angenommen wird, nicht eingetreten ist, musste bei der Erstellung der nachfolgenden Checkliste auf die Fassung vom 13. 3. 2024 zurückgegriffen werden. Eine Checkliste für General Purpose AI Models (GPAI) bleibt einer späteren Dako-Ausgabe vorbehalten.

Prüffragen

Prüffrage	ja	nein	Akteure
ALLGEMEINES			
Frage 1: Welche der in Art 2 Abs 1 normierten Rollen trifft aus Sie zu? Anmerkung: Art 2 Abs 1 enthält differenzierte Bestimmungen, abhängig von der Rolle der verschiedenen Akteure (Anbieter, Betreiber, Einführer und Händler, Produkthersteller, Bevollmächtigte von Anbietern sowie betroffene Personen) und der Risikoeinstufung des jeweiligen KI-Systems bzw KI-Modells.			A, B, C, D, E, F
Frage 2: Wurde das von Ihnen vertriebene KI-System oder KI-Modell eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen? Anmerkung: In diesem Fall unterliegt das KI-System oder KI-Modell gem Art 2 Abs 6 nicht dem AI Act.			A, B, D
Frage 3: Führen Sie Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen durch? Anmerkung: So weit Sie diese KI-Systeme und KI-Modelle noch nicht in Verkehr gebracht oder in Betrieb genommen haben, unterliegen diese Tätigkeiten gem Art 2 Abs 8 nicht dem AI Act.			A, D
Frage 4: Sind Sie eine natürliche Person und verwenden Sie ein KI-System im Rahmen Ihrer ausschließlich persönlichen und nicht beruflichen Tätigkeit? Anmerkung: In diesem Fall kommt der AI Act gem Art 2 Abs 10 nicht zur Anwendung.			natürliche Personen
Frage 5: Werden KI-Systeme unter freien und quellenoffenen Lizenzen bereitgestellt? Anmerkung: In diesem Fall kommt der AI Act gem Art 2 Abs 12 nicht zur Anwendung.			A, B, C, D
Frage 6: Werden Maßnahmen ergriffen, um nach besten Kräften sicherzustellen, dass Mitarbeiter und andere Personen, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, ausreichend geschult sind? Anmerkung: Art 4 fordert, dass die Mitarbeiter und andere Personen, die im Auftrag der Anbieter und Betreiber KI-Systeme betreiben, über ein ausreichendes Maß an KI-Kompetenz verfügen, und zwar unter Berücksichtigung ihrer technischen Kenntnisse, ihrer Erfahrung, ihrer Ausbildung und Kontextes, in dem die KI-Systeme eingesetzt werden.			A, B
KI-SYSTEME MIT INAKZEPTABLEM RISIKO			
Frage 7: Importieren, vertreiben oder betreiben Sie ein KI-System, das gem Art 5 Abs 1 als verboten eingestuft ist? Anmerkung: Das Einführen, Vertreiben oder Betreiben solcher KI-Systeme ist nach dem AI Act grundsätzlich verboten. Ausnahmen bestehen nur in einem sehr engen Bereich, wie zB der Strafverfolgung durch die Sicherheitsbehörden. Das Verbot tritt gem Art 113 lit a sechs Monate nach Inkrafttreten des AI Act in Kraft. Die Nichtbefolgung dieses Verbots kann mit einer Geldbuße von bis zu 35 Mio Euro bzw 7% des weltweiten Jahresumsatzes (davon abhängig, welcher Wert höher ist) sanktioniert werden.			A, B, C, D, E

Prüffrage	ja	nein	Akteure
HOCHRISIKO-KI-SYSTEME			
<p>Frage 8: Ist das in Verkehr gebrachte oder in Betrieb genommene KI-System als Hochrisiko-System einzustufen?</p> <p>Anmerkung: Nach Art 6 Abs 1 lit a fallen KI-Systeme in diese Risikogruppe, wenn sie als Sicherheitskomponente eines unter die in Anh I angeführten Harmonisierungsvorschriften der EU fallenden Produkts verwendet werden bzw wenn das KI-System selbst ein solches Produkt ist. Gem Art 6 Abs 1 lit b muss ein Produkt, dessen Sicherheitskomponente das KI-System ist, einer Konformitätsbewertung gem den in Anh I aufgeführten Harmonisierungsvorschriften der EU durch Dritte unterzogen werden. Darüber hinaus gelten gem Art 6 Abs 2 die in Anh III genannten KI-Systeme als hochriskant.</p>			A, B, C, D
<p>Frage 9: Kann das in Verkehr gebrachte oder in Betrieb genommene KI-System als NICHT hochriskant eingestuft werden?</p> <p>Anmerkung: Gem Art 6 Abs 3 gilt ein KI-System als nicht hochriskant, wenn es kein erhebliches Risiko in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt und es ua nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst. Dies ist dann der Fall, wenn die Bedingungen des Art 6 Abs 3 lit a bis d erfüllt sind.</p>			A, B, C, D
<p>Frage 10: Sind Sie als Anbieter der Auffassung, dass ein von Ihnen angebotenes und im Anh III angeführtes KI-System NICHT hochriskant ist?</p> <p>Anmerkung: In diesem Fall müssen Sie gem Art 6 Abs 4, bevor das KI-System in Verkehr gebracht oder in Betrieb genommen wird, Ihre Bewertung dokumentieren. Darüber hinaus müssen Sie oder Ihr Bevollmächtigter dieses KI-System gem Art 49 Abs 2 in der in Art 71 genannten Datenbank registrieren.</p>			A, E
<p>Frage 11: Haben Sie für Ihr Hochrisiko-KI-System ein Risikomanagementsystem implementiert, das verwendet, dokumentiert und aufrechterhalten wird?</p> <p>Anmerkung: Art 9 Abs 1 fordert die Einrichtung eines Risikomanagementsystems in Bezug auf die Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können. Das Risikomanagementsystem ist gem Art 9 Abs 2 als kontinuierlicher iterativer Prozess einzurichten und über den gesamten Lebenszyklus des KI-Systems zu betreiben. Art 9 Abs 2 lit a bis d beschreibt die bekannten Schritte eines Risikomanagementsystems wie Risikoidentifikation, Risikoanalyse, Risikobeurteilung, Risikominderung und Risikoüberwachung.</p>			A, B, D, E
<p>Frage 12: Werden Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, nur mit Trainings-, Validierungs- und Testdatensätzen entwickelt, die den in Art 10 Abs 2 normierten Daten-Governance- und Datenverwaltungsverfahren entsprechen?</p> <p>Anmerkung: Art 10 Abs 2 bis 5 enthalten die detaillierten Anforderungen an die Daten-Governance- und Datenverwaltungsverfahren, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind. Dazu zählen ua Untersuchungen in Hinblick auf mögliche Bias, die die Gesundheit und Sicherheit von Personen beeinträchtigen sowie sich negativ auf die Grundrechte auswirken, die Ermittlung relevanter Datenlücken sowie zusätzlich zu den Bestimmungen der VO (EU) 2016/679, der RL (EU) 2016/680 sowie der VO (EU) 2018/1725 Bedingungen für die ausnahmsweise Verarbeitung besonderer Kategorien personenbezogener Daten.</p>			A, B, D
<p>Frage 13: Liegt eine technische Dokumentation des Hochrisiko-KI-Systems vor?</p> <p>Anmerkung: Gem Art 11 ist vor Inverkehrbringen oder Inbetriebnahme des Hochrisiko-KI-Systems eine technische Dokumentation zu erstellen, die die in Anh IV genannten Angaben enthält. Diese Dokumentation soll den zuständigen nationalen Behörden und den notifizierten Stellen ermöglichen zu beurteilen, ob das KI-System die Anforderungen des Kapitel III Abschnitt 2 (Art 8 bis 15) erfüllt. Die technische Dokumentation ist gem Art 18 Abs 1 lit a vom Anbieter zehn Jahre aufzubewahren.</p>			A, B, D
<p>Frage 14: Ermöglicht die Technik des Hochrisiko-KI-Systems die automatische Protokollierung von Ereignissen während des gesamten Lebenszyklus?</p> <p>Anmerkung: Art 12 Abs 1 fordert die automatische Aufzeichnung von Ereignissen zur Gewährleistung der Funktionsfähigkeit des Hochrisiko-KI-Systems. In Art 12 Abs 3 wird der Mindestumfang der Protokollierungsfunktion beschrieben. Dieses Protokoll ist vom Anbieter gem Art 19 Abs 1 sechs Monate aufzubewahren.</p>			A, B, D
<p>Frage 15: Liegt für das Hochrisiko-KI-System eine Gebrauchsanweisung in einem geeigneten digitalen Format vor?</p> <p>Anmerkung: Art 13 Abs 1 fordert, dass Hochrisiko-KI-Systeme so konzipiert und entwickelt werden, dass ihr Betrieb hinreichend transparent ist und die Betreiber die Ergebnisse eines Systems angemessen interpretieren können. Zum Nachweis dieser Anforderung ist eine Gebrauchsanweisung zu erstellen, die mindestens die in Art 13 Abs 3 angeführten Informationen enthält.</p>			A, D
<p>Frage 16: Kann das Hochrisiko-KI-System von natürlichen Personen wirksam beaufsichtigt werden?</p> <p>Anmerkung: Hochrisiko-KI-Systeme müssen gem Art 14 so konzipiert und entwickelt sein, dass natürliche Personen ihre Funktionsweise überwachen und sicherstellen können. Zu diesem Zweck sollte der Anbieter des Systems geeignete Maßnahmen für die menschliche Aufsicht festlegen und das KI-System über Mechanismen verfügen, die es einer natürlichen Person ermöglichen, das System abzuschalten.</p>			A, B, D
<p>Frage 17: Erreicht das Hochrisiko-KI-System ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit?</p> <p>Anmerkung: Art 15 Abs 3 fordert die Angabe der Maße an Genauigkeit und von Genauigkeitskennzahlen in der Gebrauchsanweisung, in Abs 4 das Treffen von technischen und organisatorischen Maßnahmen zur Sicherstellung der Widerstandsfähigkeit sowie in Abs 5 die Gewährleistung der Cybersicherheit, die den jeweiligen Umständen und Risiken angemessen sind.</p>			A, B, D
<p>Frage 18: Erfüllen der Anbieter und der Betreiber die in Art 16 normierten Pflichten?</p> <p>Anmerkung: Art 16 lit a bis l enthält die vom Anbieter und Betreiber von Hochrisiko-KI-Systemen zu erfüllenden Pflichten wie</p> <ul style="list-style-type: none"> - Angabe ihrer Kontaktdaten, - des eingetragenen Handelsnamens bzw der eingetragenen Handelsmarke auf dem Hochrisiko-KI-System selbst oder auf der Verpackung, - die Implementierung eines Qualitätsmanagementsystems, - die Unterziehung des KI-Systems unter das in Art 43 normierte Konformitätsbewertungsverfahren, - die Ausstellung einer EU-Konformitätserklärung gem Art 47, - die CE-Kennzeichnung gem Art 48, - die Erfüllung der in Art 49 Abs 1 vorgeschriebenen Registrierungspflichten, - das Ergreifen der erforderlichen Korrekturmaßnahmen und Bereitstellung der Informationen gem Art 20 sowie - die Sicherstellung, dass das KI-System die Barrierefreiheitsanforderungen gem RL 2016/2102/EU und RL (EU) 2019/882 erfüllt. 			A, B

die checkliste

Prüffrage	ja	nein	Akteure
<p>Frage 19: Wurde vom Anbieter des Hochrisiko-KI-Systems ein Qualitätsmanagementsystem implementiert? Anmerkung: Anbieter von Hochrisiko-KI-Systemen müssen gem Art 17 Abs 1 ein Qualitätsmanagementsystem betreiben, das die Anforderungen der lit a bis m erfüllt. Die Dokumentation ist gem Art 18 lit b zehn Jahre aufzubewahren.</p>			A, B
<p>Frage 20: Ist sichergestellt, dass der Anbieter bei Annahme, dass das von ihm in Verkehr gebrachte oder in Betrieb genommene Hochrisiko-KI-System nicht den Anforderungen des AI Act entspricht, entsprechende Maßnahmen gesetzt? Anmerkung: Gem Art 20 Abs 1 hat der Anbieter in diesem Fall unverzüglich entsprechende Korrekturmaßnahmen zu setzen oder das System zu deaktivieren oder zurückzurufen. Birgt das Hochrisiko-KI-System ein Risiko iSd Art 79 Abs 1 (Anm: das sind Risiken für die Gesundheit, Sicherheit oder Grundrechte von Personen), hat der Anbieter unverzüglich und gegebenenfalls mit dem Betreiber eine Untersuchung durchzuführen und die zuständige notifizierte Stelle in Übereinstimmung mit den Bestimmungen des Art 44 zu informieren.</p>			A
<p>Frage 21: Ist sichergestellt, dass der Anbieter eines Hochrisiko-KI-Systems einer Behörde auf deren begründete Anfrage alle Informationen zur Verfügung stellen kann, um die Konformität des Systems nachweisen zu können? Anmerkung: Art 21 fordert vom Anbieter die Sicherstellung der Zusammenarbeit mit den zuständigen Behörden durch Übermittlung aller Informationen und Dokumentationen auf deren begründete Anforderung sowie gegebenenfalls gem Abs 2 auch den Zugang zu den vom Anbieter gem Art 12 erzeugten Protokollen.</p>			A
<p>Frage 22: Wurde vom Anbieter, der in einem Drittstaat niedergelassen ist, ein in der EU niedergelassener Bevollmächtigter ernannt? Anmerkung: Art 22 fordert von einem in einem Drittstaat niedergelassenen Anbieter die Ernennung eines in der EU niedergelassenen Bevollmächtigten, der im Auftrag des Anbieters die unter Abs 3 lit a bis e angeführten Aufgaben wahrnimmt. Damit soll sichergestellt werden, dass eine in der EU niedergelassene Person den Behörden die erforderlichen Informationen liefert.</p>			A, E
<p>Frage 23: Beachten Sie als Einführer (Importeur) die Ihnen vom AI Act auferlegten Pflichten? Anmerkung: Art 23 Abs 1 fordert vom Einführer (Importeur) die Prüfung des Hochrisiko-KI-Systems, bevor er dieses einführt. Darunter fallen die Überprüfung, ob ein Konformitätsbewertungsverfahren gem Art 43 vorliegt, die technische Dokumentation gem Art 11 und Anh IV erstellt wurde, das System mit der erforderlichen CE-Kennzeichnung versehen ist und ob die EU-Konformitätserklärung und die Gebrauchsanweisungen beigefügt sind sowie ein Bevollmächtigter gem Art 22 Abs 1 ernannt wurde. Weitere Pflichten ergeben sich aus den Abs 2 bis 7.</p>			C
<p>Frage 24: Beachten Sie als Händler die Ihnen vom AI Act auferlegten Pflichten? Anmerkung: Den Händler treffen die in Art 24 normierten Pflichten bevor er ein Hochrisiko-KI-System auf dem Markt bereitstellt. So muss er überprüfen, ob das System eine CE-Kennzeichnung aufweist, ob die Konformitätserklärung und die Gebrauchsanweisungen zur Verfügung stehen. Stellt er fest, dass das Hochrisiko-KI-System nicht den Anforderungen entspricht, so bietet er das System erst nach Herstellung der Konformität an bzw nimmt es zurück oder ruft es zurück. Birgt das System ein Risiko in Bezug auf die Gesundheit, Sicherheit und Grundrechte, so informiert er unverzüglich den Anbieter bzw den Einführer (Importeur). Darüber hinaus ist er auch verpflichtet, mit den Behörden zusammenzuarbeiten.</p>			C
<p>Frage 25: Beachten Sie als Betreiber die Ihnen vom AI Act auferlegten Pflichten? Anmerkung: Den Betreiber treffen gem Art 26 sehr umfangreiche Pflichten. Va hat er gem Abs 1 geeignete technische und organisatorische Maßnahmen zu treffen, sicherzustellen, dass das Hochrisiko-KI-System entsprechend der Gebrauchsanweisung verwendet wird und dass gem Abs 2 die Mitarbeiter, die die Aufsicht wahrnehmen, über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, gem Abs 4 dafür zu sorgen, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen, sowie gem Abs 5 den Betrieb zu überwachen.</p>			B
KI-SYSTEME MIT BEGRENZTEM RISIKO			
<p>Frage 26: Stellen Sie als Anbieter sicher, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, die entsprechenden Transparenzpflichten des Art 50 erfüllen? Anmerkung: Art 50 fordert, dass natürliche Personen angemessen informiert werden, dass sie mit einer Künstlichen Intelligenz interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person offensichtlich.</p>			A, B, D

Dako 2024/29

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH und fachkundiger Laienrichter für Datenschutz am BVwG. E-Mail: hj.pollirer@secur-data.at

Links

AI Act vs ChatGPT – ein spannendes Match. Kann die rechtliche Regulierung von KI-Systemen mit der technischen Entwicklung Schritt halten? Darüber sprechen Lena Urban und Gerald Trieb (beide Knyrim Trieb Rechtsanwälte) in dieser Episode mit Elisabeth Maier (MANZ): www.manz.at/rechtaktuell/podcast (S 2:E 5)