

KI-VO

Martini / Wendehorst

2024

ISBN 978-3-406-81136-4

C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.

beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

2. Betroffene Vorschriften. Von der Öffnungsklausel in Art. 2 Abs. 11 unmittelbar betroffen sind nur Vorschriften, die **für Arbeitnehmer** im Hinblick auf den Schutz ihrer Rechte bei der Verwendung von KI-Systemen durch die Arbeitgeber **günstiger** sind. Wie auch sonst bei ähnlichen Öffnungsklauseln gegenüber Rechtsvorschriften oder privatautonomer Gestaltung wird man dies in formalem und individuellem Sinne verstehen müssen, dh es kommt nicht darauf an, was unter Berücksichtigung aller Auswirkungen auf den Arbeitsmarkt und die anzunehmende persönliche Entwicklung von Arbeitnehmern (möglicherweise) am Ende für diese „besser“ ist, sondern primär darauf, was Arbeitnehmern mehr Rechte gegenüber den Arbeitgebern gibt bzw. was die Arbeitgeber in ihren **Gestaltungs- und Weisungsbefugnissen** gegenüber Arbeitnehmern einschränkt. Betroffen sind vor allem KI-Systeme zum Screening von Bewerbungen, zur Zeiterfassung oder zur Leistungsbemessung. 152

Zu berücksichtigen ist, dass Art. 2 Abs. 11 nur Vorschriften anspricht, welche im Hinblick auf den Schutz von Arbeitnehmerrechten bei der **Verwendung** von KI-Systemen durch die Arbeitgeber günstiger sind. Keinesfalls können sich Mitgliedstaaten auf die Öffnungsklausel stützen, um auch das Inverkehrbringen oder die Inbetriebnahme (iSd Art. 3 Nr. 11) von KI-Systemen für den Arbeitsbereich abweichend von der KI-VO zu regeln. 153

III. Abschließende Harmonisierung der Verwendung von KI-Systemen durch die KI-VO?

Der zuletzt genannte Punkt lenkt den Blick auf ein generelles Problem mit Art. 2 Abs. 11. Die „Öffnungsklausel“ scheint nämlich zu suggerieren, dass ohne sie die Mitgliedstaaten nicht befugt wären, die Verwendung von KI-Systemen im Arbeitsbereich zu regeln. Das wirft die Frage auf, inwieweit die KI-VO überhaupt eine **Harmonisierung im Hinblick auf die Zulässigkeit reiner Verwendung** von KI-Systemen vornimmt, dh auf die Zulässigkeit einer Verwendung, die nicht nur als Annex zu Inverkehrbringen und Inbetriebnahme geregelt ist, sondern um ihrer selbst willen. 154

Eine **Sperrwirkung** für mitgliedstaatliche Vorschriften kann die KI-VO nur entfalten, soweit die mitgliedstaatlichen Vorschriften mit den Vorschriften der KI-VO funktionell konkurrieren. Das betrifft Vorschriften, die erstens speziell oder zumindest primär KI-Systeme iSd Art. 3 Nr. 1 KI-VO betreffen, zweitens den Regelungsinhalten der KI-VO funktionell entsprechende oder mit ihnen unvereinbare Bestimmungen enthalten (insbesondere absolute Verbote des Inverkehrbringens, der Inbetriebnahme und der Verwendung von KI-Systemen, Anforderungen an die Entwicklung und das Design von KI-Systemen oder Transparenzvorschriften), und dies drittens überwiegend oder zumindest auch mit dem Ziel, Risiken für Gesundheit, Sicherheit und Grundrechte hintanzuhalten. 155

Ohne die Öffnungsklausel wäre es Mitgliedstaaten also **beispielsweise** tatsächlich verwehrt, im nationalen Recht das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen für das Screening von Bewerbungen absolut mit der Begründung zu verbieten, dass solche Systeme die Gefahr von Diskriminierung schaffen.¹⁰¹ Die KI-VO kann aber kaum etwa einer mitgliedstaatlichen Verwaltungsvorschrift entgegenstehen, welche für den Bereich der staatlichen Verwaltung anordnet, dass Bewerbungen um freie Stellen ausschließlich von Menschen bewertet werden dürfen, um eine hohe Qualität des Auswahlprozesses und das Vertrauen der Bevölkerung in die Zuverlässigkeit von Stellenbesetzungen zu stärken. Ebenso wenig kann angenommen werden, dass die Mitgliedstaaten wegen Art. 5 Abs. 1 lit. f und Anhang III Nr. 3 KI-VO die Verwendung von KI im Bildungssektor (zB die Zulassung der Nutzung von ChatGPT bei Abschlussprüfungen) nicht mehr regeln dürften, etwa mit dem Ziel, die Ausbildung zu verbessern. 156

¹⁰¹ Dies deswegen, weil das Screening von Bewerbungen nur nach Art. 6 Abs. 2 mit Annex III Punkt 4 lit. a als Hochrisiko-KI-System, aber nicht als verbotenes KI-System nach Art. 5 Abs. 1 eingestuft ist, und weil es sich bei Diskriminierung um eine Gefahr für die Grundrechte handelt.

- 157 Generell dürfte man bei mitgliedstaatlichen Regelungen, die nur eine bestimmte Verwendung, nicht aber zugleich auch das Inverkehrbringen und die Inbetriebnahme verbieten, eine Sperrwirkung verneinen müssen, wenn die mitgliedstaatlichen Regelungen entweder **gar nicht speziell KI-Systeme** adressieren oder ganz andere, von der KI-VO **nicht abschließend erwogene Schutzzwecke** verfolgen oder speziell die **eigenen staatlichen Stellen** betreffen (vgl. auch → Art. 5 Rn. 192 ff.). Art. 2 Abs. 11 lässt damit nicht ohne weiteres Rück- oder gar Umkehrschlüsse auf andere Sektoren zu.

Art. 3* Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „KI-System“ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können;
2. „Risiko“ die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens;
3. „Anbieter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;
4. „Betreiber“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;
5. „Bevollmächtigter“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;
6. „Einführer“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;
7. „Händler“ eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;
8. „Akteur“ einen Anbieter, Produkthersteller, Betreiber, Bevollmächtigten, Einführer oder Händler;
9. „Inverkehrbringen“ die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt;
10. „Bereitstellung auf dem Markt“ die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit;
11. „Inbetriebnahme“ die Bereitstellung eines KI-Systems in der Union zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung;

* Kapitel I (Art. 1–4) gilt gem. Art. 113 Abs. 3 Buchst. a bereits ab 2.2.2025.

12. „Zweckbestimmung“ die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation;
13. „vernünftigerweise vorhersehbare Fehlanwendung“ die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen, auch anderen KI-Systemen, ergeben kann;
14. „Sicherheitsbauteil“ einen Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet;
15. „Betriebsanleitungen“ die Informationen, die der Anbieter bereitstellt, um den Betreiber insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI-Systems zu informieren;
16. „Rückruf eines KI-Systems“ jede Maßnahme, die auf die Rückgabe an den Anbieter oder auf die Außerbetriebsetzung oder Abschaltung eines den Betreibern bereits zur Verfügung gestellten KI-Systems abzielt;
17. „Rücknahme eines KI-Systems“ jede Maßnahme mit der die Bereitstellung eines in der Lieferkette befindlichen KI-Systems auf dem Markt verhindert werden soll;
18. „Leistung eines KI-Systems“ die Fähigkeit eines KI-Systems, seine Zweckbestimmung zu erfüllen;
19. „notifizierende Behörde“ die nationale Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist;
20. „Konformitätsbewertung“ ein Verfahren mit dem bewertet wird, ob die in Titel II Abschnitt 2 festgelegten Anforderungen an ein Hochrisiko-KI-System erfüllt wurden;
21. „Konformitätsbewertungsstelle“ eine Stelle, die Konformitätsbewertungstätigkeiten einschließlich Prüfungen, Zertifizierungen und Inspektionen durchführt und dabei als Dritte auftritt;
22. „notifizierte Stelle“ eine Konformitätsbewertungsstelle, die gemäß dieser Verordnung und den anderen einschlägigen Harmonisierungsrechtsvorschriften der Union notifiziert wurde;
23. „wesentliche Veränderung“ eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde;
24. „CE-Kennzeichnung“ eine Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System die Anforderungen erfüllt, die in Kapitel III Abschnitt 2 und in anderen anwendbaren Harmonisierungsrechtsvorschriften, die die Anbringung dieser Kennzeichnung vorsehen, festgelegt sind;
25. „System zur Beobachtung nach dem Inverkehrbringen“ alle Tätigkeiten, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Erfahrungen mit der Verwendung der von ihnen in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmaßnahmen zu ergreifen sind;
26. „Marktüberwachungsbehörde“ die nationale Behörde, die die Tätigkeiten durchführt und die Maßnahmen ergreift, die in der Verordnung (EU) 2019/1020 vorgesehen sind;

27. „harmonisierte Norm“ eine harmonisierte Norm im Sinne des Artikels 2 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012;
28. „gemeinsame Spezifikation“ eine Reihe technischer Spezifikationen im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012, deren Befolgung es ermöglicht, bestimmte Anforderungen der vorliegenden Verordnung zu erfüllen;
29. „Trainingsdaten“ Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden;
30. „Validierungsdaten“ Daten, die zur Evaluation des trainierten KI-Systems und zur Einstellung seiner nicht erlernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Unter- oder Überanpassung zu vermeiden;
31. „Validierungsdatensatz“ einen separaten Datensatz oder einen Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung;
32. „Testdaten“ Daten, die für eine unabhängige Bewertung des KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen;
33. „Eingabedaten“ die in ein KI-System eingespeisten oder von diesem direkt erfassten Daten, auf deren Grundlage das System eine Ausgabe hervorbringt;
34. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische Daten;
35. „biometrische Identifizierung“ die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind;
36. „biometrische Verifizierung“ die automatisierte Eins-zu-eins-Verifizierung, einschließlich Authentifizierung, der Identität natürlicher Personen durch den Vergleich ihrer biometrischen Daten mit zuvor bereitgestellten biometrischen Daten;
37. „besondere Kategorien personenbezogener Daten“ die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, Artikel 10 der Richtlinie (EU) 2016/680 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 aufgeführten Kategorien personenbezogener Daten;
38. „sensible operative Daten“ operative Daten im Zusammenhang mit Tätigkeiten zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten, deren Offenlegung die Integrität von Strafverfahren gefährden könnte;
39. „Emotionserkennungssystem“ ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten;
40. „System zur biometrischen Kategorisierung“ ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien zuzuordnen, sofern es sich um eine Nebenfunktion eines anderen kommerziellen Dienstes handelt und aus objektiven technischen Gründen unbedingt erforderlich ist;
41. „biometrisches Fernidentifizierungssystem“ ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren;
42. „biometrisches Echtzeit-Fernidentifizierungssystem“ ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, und das zur Vermeidung einer Umgehung der Vorschriften nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen umfasst;

43. „System zur nachträglichen biometrischen Fernidentifizierung“ ein biometrisches Fernidentifizierungssystem, das kein biometrisches Echtzeit-Fernidentifizierungssystem ist;
44. „öffentlich zugänglicher Raum“ einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort in privatem oder öffentlichem Eigentum, unabhängig davon, ob bestimmte Bedingungen für den Zugang gelten, und unabhängig von möglichen Kapazitätsbeschränkungen;
45. „Strafverfolgungsbehörde“:
 - a) eine Behörde, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder
 - b) eine andere Stelle oder Einrichtung, der durch nationales Recht die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;
46. „Strafverfolgung“ Tätigkeiten der Strafverfolgungsbehörden oder in deren Auftrag zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
47. „Büro für Künstliche Intelligenz“ die Aufgabe der Kommission, zur Umsetzung, Beobachtung und Überwachung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck und zu der im Beschluss der Kommission vom 24. Januar 2024 vorgesehenen KI-Governance beizutragen; Bezugnahmen in dieser Verordnung auf das Büro für Künstliche Intelligenz gelten als Bezugnahmen auf die Kommission;
48. „zuständige nationale Behörde“ eine notifizierende Behörde oder eine Marktüberwachungsbehörde; in Bezug auf KI-Systeme, die von Organen, Einrichtungen und sonstigen Stellen der Union in Betrieb genommen oder verwendet werden, sind Bezugnahmen auf die zuständigen nationalen Behörden oder Marktüberwachungsbehörden in dieser Verordnung als Bezugnahmen auf den Europäischen Datenschutzbeauftragten auszulegen;
49. „schwerwiegender Vorfall“ einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:
 - a) den Tod oder die schwere gesundheitliche Schädigung einer Person;
 - b) eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen;
 - c) die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte;
 - d) schwere Sach- oder Umweltschäden;
50. „personenbezogene Daten“ personenbezogene Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;
51. „nicht personenbezogene Daten“ Daten, die keine personenbezogenen Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679 sind;
52. „Profiling“ das Profiling im Sinne von Artikel 4 Nummer 4 der Verordnung (EU) 2016/679;
53. „Plan für einen Test unter Realbedingungen“ ein Dokument, in dem die Ziele, die Methodik, der geografische, bevölkerungsbezogene und zeitliche Umfang, die Überwachung, die Organisation und die Durchführung eines Tests unter Realbedingungen beschrieben werden;
54. „Plan für das Reallabor“ ein zwischen dem teilnehmenden Anbieter und der zuständigen Behörde vereinbartes Dokument, in dem die Ziele, die Bedingungen, der Zeitrahmen, die Methodik und die Anforderungen für die im Reallabor durchgeführten Tätigkeiten beschrieben werden;

55. „KI-Reallabor“ einen kontrollierten Rahmen, der von einer zuständigen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter Realbedingungen – zu testen.
56. „KI-Kompetenz“ die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden.
57. „Test unter Realbedingungen“ den befristeten Test eines KI-Systems auf seine Zweckbestimmung, der unter Realbedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung erfolgt, um zuverlässige und belastbare Daten zu erheben und die Konformität des KI-Systems mit den Anforderungen der vorliegenden Verordnung zu bewerten und zu überprüfen, wobei dieser Test nicht als Inverkehrbringen oder Inbetriebnahme des KI-Systems im Sinne dieser Verordnung gilt, sofern alle Bedingungen nach Artikel 57 oder Artikel 60 erfüllt sind;
58. „Testteilnehmer“ für die Zwecke eines Tests unter Realbedingungen eine natürliche Person, die an dem Test unter Realbedingungen teilnimmt;
59. „informierte Einwilligung“ eine aus freien Stücken erfolgende, spezifische, eindeutige und freiwillige Erklärung der Bereitschaft, an einem bestimmten Test unter Realbedingungen teilzunehmen, durch einen Testteilnehmer, nachdem dieser über alle Aspekte des Tests, die für die Entscheidungsfindung des Testteilnehmers bezüglich der Teilnahme relevant sind, aufgeklärt wurde;
60. „Deepfake“ einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde;
61. „weitverbreiteter Verstoß“ jede Handlung oder Unterlassung, die gegen das Unionsrecht verstößt, das die Interessen von Einzelpersonen schützt, und die
- a) die kollektiven Interessen von Einzelpersonen in mindestens zwei anderen Mitgliedstaaten als dem Mitgliedstaat schädigt oder zu schädigen droht, in dem
 - i) die Handlung oder die Unterlassung ihren Ursprung hatte oder stattfand,
 - ii) der betreffende Anbieter oder gegebenenfalls sein Bevollmächtigter sich befindet oder niedergelassen ist oder
 - iii) der Betreiber niedergelassen ist, sofern der Verstoß vom Betreiber begangen wird;
 - b) die kollektiven Interessen von Einzelpersonen geschädigt hat, schädigt oder schädigen könnte und allgemeine Merkmale aufweist, einschließlich derselben rechtswidrigen Praxis oder desselben verletzten Interesses, und gleichzeitig auftritt und von demselben Akteur in mindestens drei Mitgliedstaaten begangen wird;
62. „kritische Infrastrukturen“ kritische Infrastrukturen im Sinne von Artikel 2 Nummer 4 der Richtlinie (EU) 2022/2557;
63. „KI-Modell mit allgemeinem Verwendungszweck“: ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden;
64. „Fähigkeiten mit hoher Wirkkraft“ bezeichnet Fähigkeiten, die den bei den fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen;

65. „systemisches Risiko“ ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;
66. „KI-System mit allgemeinem Verwendungszweck“ ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen;
67. „Gleitkommaoperation“ jede Rechenoperation oder jede Zuweisung mit Gleitkommazahlen, bei denen es sich um eine Teilmenge der reellen Zahlen handelt, die auf Computern typischerweise durch das Produkt aus einer ganzen Zahl mit fester Genauigkeit und einer festen Basis mit ganzzahligem Exponenten dargestellt wird;
68. „nachgelagerter Anbieter“ einen Anbieter eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das ein KI-Modell integriert, unabhängig davon, ob das KI-Modell von ihm selbst bereitgestellt und vertikal integriert wird oder von einer anderen Einrichtung auf der Grundlage vertraglicher Beziehungen bereitgestellt wird.

Erwägungsgründe: 12 bis 19

Literatur: Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ WP 136, 2006; Artikel-29-Datenschutzgruppe, Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), WP 131, 2007; Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 2017; Ballegooij/Bakowski, The Fight Against Terrorism: Cost of Non-Europe Report, 2018; Barocas/Selbst, Big Data's Disparate Impact, CLR 2016, 671; Baumann, Generative KI und Urheberrecht – Urheber und Anwender im Spannungsfeld, NJW 2023, 3673; Borges, IT und Software: Der Begriff des KI-Systems, CR 2023, 706; Botta, Die Förderung innovativer KI-Systeme in der EU, ZfDR 2022, 391; Brey, Ethical aspects of facial recognition systems in public places Journal of Information, Communication and Ethics in Society Vol. 2 No. 2, 97; Datenethikkommission der Bundesregierung, Gutachten der Datenethikkommission, 2019; Denga, Unternehmenshaftung für KI – zur Konformitätsbewertung in Permanenz, CR 2023, 277; Denga, Konformitätsbewertung von KI-Systemen, ZfPC 2023, 154; Dornis, Der Schutz künstlicher Kreativität im Immaterialgüterrecht, GRUR 2019, 1252; Ebers, Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RD i 2021, 588; Ebert/Spiecker gen. Döhmann, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188; Ernst, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110; Etzkorn, Bedeutung der „Entwicklungslücke“ bei selbstlernenden Systemen, MMR 2020, 360; Freidewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022; Fuster, Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights, 2020; Grady, The AI Act should be Technology-Neutral, 2024; GPAI, Data Governance Working Group: A Framework Paper for GPAI's work on Data Governance, 2022; Heine, Generative KI: Nutzungsrechte und Nutzungsvorbehalt, GRUR-Prax 2024, 87; Helberger/Micklitz/Rott, EU Consumer Protection 2.0 – The Regulatory Gap: Consumer Protection in The Digital Economy, 2021, S. 29 f.; Helberger/Lynskey/Micklitz/Rott/Sax/Strycharz, EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets, 2021, S. 5 ff; Hildebrandt/Gutwirth, Profiling the European Citizen Biometric Profiling, 2010; Hinderks, Die Kennzeichnungspflicht von Deepfakes, ZUM 2022, 110; Hörauf, Ordnungswidrigkeiten und der europäische Straftatensbegriff – Subkategorie- oder aliud-Verhältnis?, ZIS 2013, 276; Kamecke/Körber, Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood, ECLR 2008, 330; Kieslich/Lünich, Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations, CoRR, abs/2401.13605 (2024); Kittelmann/Mössner, Die neue Europäische Maschinenverordnung, ARP 2023, 322; Liggieri/Müller/Karafyllis, Mensch-Maschine-Interaktion, 2019; Maamar, Urheberrechtliche Fragen beim Einsatz von generativen KI-Systemen, ZUM 2023, 481; Martini/Wiesehöfer, Auf dem Weg zur Regulierung von General-Purpose-AI – eine erste Bestandsaufnahme und Kritik der Regelungsentwürfe, NVwZ 2024, 137; McMahan/Ramage, Federated Learning: Collaborative Machine Learning without Centralized Training Data, 2017; McMahan/Moore/Ramage/Hampson/Arcas, Communication-Efficient Learning of Deep Networks from Decentralized Data, 2017; Mehlinger, Reichweite und Begrenzung des Maschinenbegriffs, InTer, 2018, 76; Mordini/Tzovaras, Second Generation Biometrics, 2012; Mühlhof/Ruscheimer, Predictive analytics and the collective dimensions of data protection, Law, Innovation and Technology, 2024; Müller-Peltzer/Tanczik, Künstliche Intelligenz und Daten, RD i 2023, 452; Muttach/Link, Verarbeitung personen-

bezogener Daten in KI-Reallaboren nach dem KI-VO-E, CR 2023, 725; Nordemann, Generative Künstliche Intelligenz: Urheberrechtsverletzungen und Haftung, GRUR 2024, 1; Obaidat/Traore/Woungang, Biometric-Based Physical and Cybersecurity Systems, 2019; OECD, Empfehlung des Rats zu künstlicher Intelligenz, 2019; OECD, Künstliche Intelligenz in der Gesellschaft, 2020; OECD, Explanatory memorandum on the updated OECD definition of an AI system, 2024; Pesch/Böhme, Artpocalypse now? – Generative KI und die Vervielfältigung von Trainingsbildern, GRUR 2023, 997; Qiang, The Road to Digital Unfreedom: President Xi’s Surveillance State, Journal of Democracy vol. 30 no. 1, 53; Rockstroh/Kunkel, IT-Sicherheit in Produktionsumgebungen, MMR 2017, 77; Roth-Isigkeit, Grundstrukturen der geplanten KI-Aufsichtsbehörden – KI-Bürokratie?, ZRP 2022, 187; Runte/Potnecke, Anwendbarkeit und Auswirkungen des Geräte- und Produktsicherheitsgesetzes auf Hersteller und Händler von Computerprogrammen, CR 2004, 725; Ruschemeier, Thinking Outside the Box? Regulatory Sandboxes as a Tool for AI Regulation, SSRN 2024, 1; Schuett, Risk Management in the Artificial Intelligence Act, EJRR 2023, 1; Schwenke, Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach der DS-GVO, NJW 2018, 823; Spindler/Büning, Einsatz von Reallaboren (Regulatory Sandboxes), JZ 2023, 799; Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2020; Spindler, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E), CR 2021, 361; Spindler/Thorum, Die Rolle der Ko-Regulierung in der Informationsgesellschaft Handlungsempfehlung für eine digitale Ordnungspolitik, MMR-Beil 2016, 1; Steege, Definition von Künstlicher Intelligenz in Art. 3 Nr. 1 KI-VO-E, MMR 2022, 926; Stiemerling/Weiß/Wendehorst, Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG; Thiel, „Deepfakes“ – Sehen heißt glauben?, ZRP 2021, 202; Truby/Brown/Ibrahim/Parellada, A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications, EJRR 2022, 270; UNCITRAL Secretariat, Explanatory note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts, 2007; Veale/Borgesius, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97; VZBV, Artificial Intelligence needs real world regulation, 2021; Wachter/Mittelstadt/Froidi, International Data Privacy Law, 2017; Welser, Generative KI und Urheberrechtsschranken, GRUR-Prax 2023, 516; Wendehorst/Duller, Biometric Recognition and Behavioural Detection, 2021; Wendehorst/Duller, Safety and Liability Related Aspects of Software, European Commission, 2021; Wendehorst, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective, 14.12.2021; Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des KI-Systems unter der neuen KI-VO – der Drei-Faktor-Ansatz, MMR 2024, 605; Wiebe, Produktsicherheitsrechtliche Pflicht zur Bereitstellung sicherheitsrelevanter Software-Updates, NJW 2019, 625; Wiebe, Produktsicherheitsrechtliche Betrachtung des Vorschlags für eine KI-Verordnung, BB 2022, 899; Wolf, Introducing Biometric Technology in Elections, 2017; Yeom/Giacomelli/Fredrikson/Jha 2018 IEEE 31st Computer Security Foundations Symposium, 268; Zech, Künstliche Intelligenz und Haftungsfragen, ZfPW 2019, 198.

Übersicht

	Rn.
A. Allgemeines	1
B. Inhalt der Regelung	3
I. Die Definition von „KI-System“	3
1. Allgemeines	3
a) Normzweck und Bedeutung im Kontext der KI-VO	3
b) Bezüge zu anderen Rechtsakten	7
c) Leitlinien der Europäischen Kommission	13
d) Entstehungsgeschichte	14
2. Maschinengestütztes System	19
a) Abgrenzung von biologischen Systemen	19
b) Abgrenzung von anderen Produktkomponenten	22
c) Abgrenzung von bloßen KI-Modellen	25
3. Charakteristika von KI	29
a) Operation mit unterschiedlichem Grad an Autonomie	29
b) Mögliche Anpassungsfähigkeit	32
c) Erstellte Ausgaben (Output)	35
d) Ableitung aus Eingaben	43
4. Kritik und Versuch einer eigenen Systematisierung: Drei-Faktoren-Theorie	50
a) Kritische Bewertung der Definition	50
b) Die drei Faktoren	53
c) Verhältnis der drei Faktoren zueinander	56
II. Die Definitionen im Einzelnen	59
1. „KI-System“	59