KI und KI-Verordnung aus datenschutzrechtlicher Sicht

Professor Dr. Alexander Golland*

Nicht erst seit der Verabschiedung der europäischen KI-Verordnung im Mai 2024 ist das Schlagwort „Künstliche Intelligenz“ (KI) im datenschutzrechtlichen Diskurs angekommen. Doch der Einsatz von KI birgt zahlreiche datenschutzrechtliche Herausforderungen; mitunter wird KI-Einsatz insgesamt als mit dem Datenschutzrecht unvereinbar angesehen. Neben der datenschutzrechtlichen Zulässigkeit des KI-Einsatzes stellen sich bislang kaum beleuchtete Grundsatzfragen, etwa die der Verantwortlichkeit und deren Folgen – nach Inkrafttreten des Gesetzes über künstliche Intelligenz auch unter neuen Vorzeichen.

The buzzword “artificial intelligence” (AI) has been a hot topic in the data protection debate, and certainly not only since the adoption of the European AI Act in May 2024. However, the use of AI poses numerous challenges regarding data protection law; some consider the AI usage generally be incompatible with the requirements of data protection law. Besides the lawfulness of the use of AI under data protection legislation, there are fundamental questions that have hardly been addressed to date, such as data controllership and its implications – even under new circumstances after the AI Act came into force.

I. Beteiligte beim KI-Einsatz

Zahlreichen Studien lässt sich entnehmen, dass KI im Unternehmenskontext zunehmend relevant wird: Rund drei Viertel der Unternehmen wollen bis zum Jahr 2027 KI einsetzen.[1] Ungeachtet des konkreten Einsatzszenarios lassen sich regelmäßig vier Beteiligte beim Einsatz von KI ausmachen: KI-Entwickler, KI-Trainer, KI-Anbieter und KI-Nutzer.

Denkbar ist, dass im Falle einer vollständigen Eigenentwicklung und -nutzung eines KI-Tools alle vier Rollen zusammenfallen – im Regelfall existieren aber mindestens drei Beteiligte: Der KI-Entwickler, der das System bzw. dessen Algorithmen programmiert. Der KI-Trainer trainiert sodann das entwickelte Modell anhand von Sach- und/oder personenbezogenen Daten, welche aus eigenem Bestand verwendet, künstlich generiert (synthetische Daten) oder aus allgemein zugänglichen Quellen bezogen („data scraping“)[2] werden. Sowohl Programmierung als auch Training können durch dasselbe Unternehmen erfolgen; es haben sich aber bereits einige Unternehmen auf das Training fremder KI („AI Training-as-a-Service“) spezialisiert. Auf der anderen Seite stehen KI-Nutzer und der KI-Anbieter, welcher dem KI-einsetzenden Unternehmen das Produkt als cloudbasierte Softwarelösung (AI-as-a-Service – „AIaaS“) anbietet. Regelmäßig ist das Unternehmen, das die KI gegenüber dem Nutzer anbietet, zugleich der KI-Entwickler; lediglich im Falle der Auftragsprogrammierung fallen diese Rollen auseinander. Umgekehrt ist denkbar, dass der KI-Nutzer die Software selbst, dh „on premise“, betreibt; hier fallen die Rollen von KI-Anbieter und KI-Nutzer zusammen.

II. Anwendungsbereich und Adressaten

Soweit sich die datenschutzrechtliche Literatur mit dem Einsatz von KI-Systemen befasst, fokussiert sie sich überwiegend auf Fragen der Rechtmäßigkeit des Einsatzes oder der Erfüllung von Betroffenenrechten. Grundsatzfragen, etwa die des Personenbezugs oder der datenschutzrechtlichen Verantwortlichkeit, bleiben vielfach unbeleuchtet. Vor allem die letztere, komplexe Frage führte bereits zur behördlichen Forderung der Klarstellung datenschutzrechtlicher Verantwortlichkeit.[3]

1. Schutzfähige Daten

Das Datenschutzrecht – insbesondere die Datenschutz-Grundverordnung (DS-GVO) – reguliert den Umgang[4] mit personenbezogenen Daten.[5] Entscheidend für den Anwendungsbereich der DS-GVO ist vor allem, welche Daten als personenbeziehbar einzustufen sind.

a) Ein- und Ausgabedaten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[6] Auf den Wahrheitsgehalt kommt es hierbei nicht an,[7] sodass auch – für den KI-Einsatz relevant – falsche Informationen, Vermutungen und Aussagen über Wahrscheinlichkeiten erfasst werden. Eine Person ist identifiziert, wenn die Identität für den Verarbeitenden unmittelbar aus

der Information hervorgeht. Dies trifft in der Regel zu, wenn die Information derart einzigartig ist, dass sie eindeutig und objektiv einer Person zugeordnet ist,[8] etwa Ausweisdokument oder Bürgernummer (Steuer-ID). Wann eine Person als identifizierbar gilt, ist seit Jahrzehnten umstritten.[9] Nach der Rechtsprechung von EuGH[10] und EuG[11] kommt es grundsätzlich auf die Perspektive des Datenverarbeiters an, allerdings sind bei der Prüfung des Personenbezugs alle tatsächlichen und rechtlichen Mittel zu berücksichtigen, die verwendet werden könnten, um den Personenbezug herzustellen.

Unproblematisch ist eine Verarbeitung personenbezogener Daten gegeben, wenn sich Eingabedaten auf eine Person beziehen, also zB KI eingesetzt wird, um bestimmte Daten, unter denen auch personenbezogene Informationen sind, auszuwerten oder aber – für generative KI relevant – eine Handlungsanweisung des Bedieners („prompt“) personenbezogene Daten enthält. Eine Verarbeitung liegt aber auch dann vor, wenn lediglich die Ausgabedaten personenbezogen sind, zB wenn ein KI-System einen Text verfassen soll und dieser Text Informationen mit Bezug zu existierenden Personen enthält. Gerade bei Large Language Models lässt sich auch durch sorgfältige Eingaben nicht vermeiden, dass der Anwendungsbereich des Datenschutzrechts eröffnet wird.

b) Daten im KI-Modell

Problematisch ist die Frage, ob die Nutzung einer KI auch dann, wenn weder Eingabedaten noch Ausgabedaten Personenbezug aufweisen, eine Verarbeitung darstellt. Werden beim Training personenbezogene Daten (zB Kundendaten, Personenfotos oder öffentliche Informationen) genutzt, so stellt dies eine Datenverarbeitung iSd Art. 4 Nr. 2 DS-GVO dar. Einen Einfluss auf den KI-Betrieb hat dies nur dann, wenn dabei Daten in einer den Personenbezug erhaltenden Form weiterverarbeitet werden, insbesondere, wenn Inhalte in Text- oder Bildform in einem Speicher erhalten bleiben. In diesem Fall stellt der Betrieb der KI durch den Anbieter ebenso eine Verarbeitung personenbezogener Daten dar wie die Verwendung jener KI durch den KI-Nutzer.

KI-Algorithmen erkennen und speichern Muster und Gesetzmäßigkeiten in Trainingsdaten, die trainierten Netze enthalten aber idR – isoliert betrachtet – keinen Personenbezug.[12] Denkbar ist ein Personenbezug jedoch dann, wenn das Training aufgrund personenspezifisch vorselektierter Daten durchgeführt wurde, also zB eine bildgenerierende KI lediglich anhand von Bildern einer bestimmten Person trainiert worden ist und in Folge dessen nur Bilder dieser generiert.[13] Darüber hinaus können KI-Erzeugnisse den Personenbezug durch Eingaben des KI-Nutzers „erben“. Werden vom KI-Nutzer etwa personenbezogene Daten in das KI-System eingegeben, etwa zur Analyse eingegebener personenbezogener Daten oder zur Erzeugung von Informationen über eine bestimmte Person, so erbt das KI-Erzeugnis den Personenbezug des prompt. Dies dürfte den Regelfall des KI-Einsatzes in Unternehmen darstellen, wenn etwa Kundendaten analysiert, KI für Recruiting-Zwecke eingesetzt oder Unternehmensprozesse und -organisation optimiert werden sollen.

Sofern weder trainierte KI noch prompt oder der KI zur Verfügung gestellte Informationen personenbezogene Daten enthalten, findet keine Verarbeitung iSd Art. 4 Nr. 2 DS-GVO statt, sodass sich die Frage der Datenschutzkonformität – jedenfalls beim Einsatz der KI – erübrigt.

2. Datenschutzrechtliche Verantwortlichkeit des KI-Nutzers

Das Datenschutzrecht kennt zwei Adressaten: Den Verantwortlichen als Primäradressat; daneben den Auftragsverarbeiter, der als „verlängerter Arm des Verantwortlichen“[14] streng weisungsgebunden tätig ist, nicht über Zwecke der Verarbeitung bestimmt und Adressat nur weniger gesetzlicher Pflichten ist. Die zentralen Pflichten richten sich vielmehr an Verantwortliche, sodass eine Befassung mit der Verteilung der datenschutzrechtlichen Rollen essenziell ist.

a) KI in eigener Verantwortlichkeit

Der einfachste, in der Praxis jedoch selten anzutreffende Fall, ist das Betreiben und die Optimierung der KI durch das KI-nutzende Unternehmen selbst. In einer solchen „on premise“-Nutzungssituation ist der KI-Nutzer allein Verantwortlicher.

b) KI im Rahmen der Auftragsverarbeitung (AI-as-a-Service)

KI-Dienstleistungen werden häufig als AIaaS angeboten. Die in Art. 4 Nr. 8 DS-GVO angelegte Rechtsfigur der Auftragsverarbeitung hat aus Nutzersicht gewisse Vorteile: Als Verantwortlicher bedarf es bei AIaaS keiner gesonderten Rechtsgrundlage für den Einsatz der Dienste des Auftragsverarbeiters; die Rechtsgrundlage des Verantwortlichen erstreckt sich vielmehr auch auf dessen Tätigkeiten,[15] was die Einbindung externer Dienste vereinfacht. Ebenso ist dies aus Sicht des AIaaS-Anbieters attraktiv, da dieser lediglich wenige Pflichten einhalten muss, die sich im Wesentlichen aus der zwischen KI-Anbieter und KI-Nutzer zu schließenden Auftragsverarbeitungsvereinbarung (Art. 28 III DS-GVO) ergeben. Verantwortlicher bleibt insoweit allein der KI-Nutzer.

Allerdings ist Wesen der Auftragsverarbeitung, dass der Auftragsverarbeiter rein weisungsabhängig für einen Verantwortlichen tätig wird.[16] Eine Verfolgung eigener Zwecke durch den vermeintlichen Auftragsverarbeiter sprengt den Rahmen und führt zur eigenen Verantwortlichkeit.[17] Problematisch ist dabei, welche Verarbeitung zu „eigenen“ Zwecken noch im Rahmen eines AIaaS-Angebots erfolgen kann. Unstreitig dürfte die Verarbeitung von vom Verantwortlichen erhaltenen Daten zur Erfüllung eigener gesetzlicher Pflichten, zB die Gewährleistung der Datensicherheit, die Grenzen einer Auftragsverarbeitung nicht überschrei-

ten.[18] Schwierigkeiten bereitet vor allem die Optimierung der angebotenen KI-Dienstleistung unter Nutzung personenbezogener Daten.[19] Wird eine KI ausschließlich anhand der vom Verantwortlichen erhaltenen Nutzungsdaten zur laufenden Verbesserung für den Verantwortlichen (weiter-)trainiert, dürfte dies wohl unproblematisch sein.[20]

c) Getrennte und gemeinsame Verantwortlichkeit

Verwendet der KI-Anbieter die von seinen Kunden erhaltenen Daten auch zur Erstellung einer verbesserten Nachfolgeversion, entsteht hinsichtlich dieser Verarbeitung eine eigene Verantwortlichkeit des KI-Anbieters. Rechtlich handelt es sich dabei um ein anerkanntes[21] Nebeneinander von Auftragsverarbeitung und getrennter Verantwortlichkeit.

Probleme bereitet schließlich die – in der Praxis durchaus übliche – tenant-übergreifende Optimierung, dh wenn der KI-Anbieter die von den KI-einsetzenden Unternehmen erhaltenen Nutzungsdaten zur laufenden Optimierung der KI für alle Kunden verwendet, sodass sowohl einzelne KI-Nutzer, als auch KI-Anbieter daraus Vorteile ziehen. In diesem Fall dürfte eine gemeinsame Verantwortlichkeit iSd Art. 4 Nr. 7 Hs. 1 Alt. 2 DS-GVO anzunehmen sein.[22] Der EuGH legt die Rechtsfigur der „gemeinsamen Verantwortlichkeit“ äußerst weit aus.[23] Ein Zugriff des KI-Nutzers auf die vom KI-Anbieter verwendeten Daten ist nicht erforderlich;[24] nach jüngster Rechtsprechung soll bereits genügen, dass die andere Stelle „aus Eigeninteresse auf die betreffende Verarbeitung Einfluss nimmt“.[25] Eine solche Einflussnahme und die damit einhergehende gemeinsame Verantwortlichkeit dürfte in vielen Fällen des Einsatzes einer fremdbetrieben KI vorliegen. Neben einer entsprechenden Rechtsgrundlage – wie im Falle getrennter Verantwortlichkeit – ist außerdem

eine Vereinbarung iSd Art. 26 I DS-GVO erforderlich. Wird diese Konstellation verkannt und etwa bloß deshalb, weil der KI-Anbieter einen Auftragsverarbeitungsvertrag anbietet,[26] eine Auftragsverarbeitung unterstellt,[27] führt dies nicht nur zu formellen Verstößen gegen die DS-GVO durch den KI-Nutzer (insbes. fehlende Dokumentation), sondern zusätzlich zum Verstoß gegen materielle Pflichten, wenn etwa die nötige Rechtsgrundlage fehlt oder Betroffenenrechte nicht gewährleistet werden.[28]

Sofern eine (teilweise) gemeinsame Verantwortlichkeit angenommen wird, befreit dies das KI-einsetzende Unternehmen nicht von Pflichten. Vielmehr bleibt es Adressat sämtlicher datenschutzrechtlicher Pflichten und haftet im Außenverhältnis auch für die in gemeinsamer Verantwortlichkeit vom KI-Anbieter durchgeführte Datenverarbeitung.[29]

d) Privater Einsatz von KI

Das Datenschutzrecht findet keine Anwendung, wenn die Verarbeitung ausschließlich zu privaten oder familiären Zwecken erfolgt (Art. 2 II Buchst. c DS-GVO). Wird ein KI-System durch eine natürliche Person zu privaten Zwecken eingesetzt und liegen die Voraussetzungen für eine Auftragsverarbeitung vor, existiert analog Art. 28 DS-GVO kein datenschutzrechtlich Verantwortlicher.[30] Dieses scheinbar unbefriedigende Ergebnis erklärt sich vor dem Hintergrund, dass der KI-Nutzer zwar über den Einsatz entscheidet, jedoch nicht Adressat des Datenschutzrechts ist; umgekehrt der KI-Anbieter nicht über die konkreten (Einsatz-)Zwecke des von ihm bereitgestellten Tools entscheidet, demnach nicht Verantwortlicher sein kann. Dies gilt gerade für „general purpose AI“, also KI-Systeme, die nicht spezifisch auf ein Einsatzszenario zugeschnitten sind. Werden die vom Privatnutzer erhaltenen oder generierten Daten hingegen vom KI-Anbieter für eigene Zwecke, etwa die KI-Optimierung, eingesetzt, so ist letzterer insoweit Verantwortlicher.

III. Spezifische Herausforderungen beim KI-Einsatz

Wenngleich die DS-GVO einen technologieneutralen Ansatz verfolgt, stellen sich beim Einsatz von KI-Systemen einige besondere Herausforderungen für Verantwortliche.

1. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Jede Datenverarbeitung beim Einsatz von KI-Systemen muss rechtmäßig erfolgen (Art. 5 I Buchst. a DS-GVO). Rechtsgrundlagen finden sich in Art. 6 I DS-GVO. Falls besondere Arten personenbezogener Daten („sensible Daten“) verarbeitet werden, bedarf es zusätzlich[31] einer Rechtsgrundlage iSd Art. 9 II DS-GVO.

a) Verarbeitung „normaler“ Daten

Eine Möglichkeit der zulässigen Datenverarbeitung ist die vorherige, informierte Einwilligung der Betroffenen (Art. 6 I UAbs. 1 Buchst. a DS-GVO). Das ist denkbar, soweit es um Daten derer geht, die selbst Daten eingeben und zu denen der Verantwortliche in Kontakt steht, etwa Kunden oder Beschäftigte.[32] Die Einwilligung ist nur wirksam, wenn diese freiwillig erteilt wurde.[33] Gerade in Abhängigkeitssituationen wie (sich anbahnenden) Beschäftigungsverhältnissen ist die Freiwilligkeit der Einwilligung zu bezweifeln;[34] eine abgegebene Einwilligungserklärung wäre dann unwirksam. Werden Daten sonstiger Betroffener eingegeben und/oder greift die KI auf das Internet zu, ist die Einholung einer vorherigen Einwilligung mangels Kontakts in der Praxis nicht umsetzbar. Werden zudem Nutzungsdaten für die Weiterentwicklung des Systems genutzt, birgt die jederzeitige Widerruflichkeit der Einwilligung[35] ein weiteres Problem: Sofern im neuronalen Netz personenbezogene Daten fortbestehen, ist eine gezielte Löschung nach Widerruf idR tech-

nisch nicht realisierbar.[36] Besteht keine Möglichkeit, die jeweiligen Daten zu isolieren und ihre Verarbeitung zu unterbinden, wäre der Einsatz des KI-Systems rechtswidrig. Auch die Anforderungen an die Informiertheit der Einwilligung sind bei dem Einsatz von KI besonders schwer zu erfüllen.[37] Insgesamt ist diese Rechtsgrundlage für den KI-Einsatz in vielen Fällen ungeeignet.

Die Datenverarbeitung ist gem. Art. 6 I UAbs. 1 Buchst. b DS-GVO auch zulässig, soweit diese erforderlich ist, um einen Vertrag zu erfüllen oder um vorvertragliche Maßnahmen auf Anfrage des Betroffenen

durchzuführen. Letzteres ist etwa beim Einsatz von Chatbots auf Websites denkbar. Dagegen scheidet die Vertragserfüllung als Rechtmäßigkeitstatbestand – ebenso wie die Einwilligung – evident aus, wenn das Unternehmen in keinem Näheverhältnis zum Betroffenen steht. In allen Konstellationen wirft aber das Kriterium der Erforderlichkeit (weitere) Probleme auf. Das „Erforderliche" ist anhand objektiver Kriterien für den jeweiligen Zweck zu bestimmen: „Erforderlichkeit" bedeutet demnach keine zwingende Notwendigkeit im Sinne einer Unmöglichkeit der Zweckerreichung ohne die beabsichtigte Datenverarbeitung, umgekehrt genügt aber die bloße Nützlichkeit der Datenverarbeitung nicht.[38] Sowohl die Europäischen Aufsichtsbehörden[39] als auch der EuGH[40] legen das Merkmal eng aus und vertreten die Ansicht, nur die für den Vertragsgegenstand objektiv notwendige Verarbeitung sei „erforderlich". Vor diesem Hintergrund kommt der KI-Einsatz auf Grundlage des Art. 6 I UAbs. 1 Buchst. b DS-GVO wohl selten in Betracht, ist aber in laufenden Beschäftigungsverhältnissen denkbar, wenn der Arbeitgeber legitime Interessen (zB Verbesserung von Kostenstruktur, Arbeitsergebnissen oder Betriebszufriedenheit) verfolgt und dabei nur geringfügig in Persönlichkeitsrechte eingreift.[41]

Schließlich ist die Verarbeitung auf Grundlage einer Interessenabwägung denkbar (Art. 6 I UAbs. 1 Buchst. f DS-GVO). Danach ist eine Verarbeitung zulässig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person demgegenüber nicht überwiegen. Der Begriff des berechtigten Interesses wird weit verstanden, sodass auch die Effizienzsteigerung bzw. Kosteneinsparung, Personalisierungsoptionen und die Optimierung der eigenen Angebote durch KI-Systeme einschließlich deren Weiterentwicklung berücksichtigungsfähig sind.[42] In der Regel dürfte – argumentum a fortiori – stets die Verarbeitung „normaler Daten" nach Art. 6 I UAbs. 1 Buchst. f DS-GVO zulässig sein, wenn ein durch Art. 9 II DS-GVO anerkanntes Szenario vorliegt, dh sogar sensible Daten rechtmäßig verarbeitet werden dürften (dazu sogleich). Auch kommt der Frage, ob der Betroffene – basierend auf dem Verhältnis zum Verantwortlichen – vernünftigerweise die Verarbeitung erwarten konnte, erhebliche Bedeutung zu.[43] Ein Beschäftigter oder (potenzieller) Kunde, der selbst Daten übermittelt, zB mit einem kenntlich gemachten Chatbot interagiert, wird regelmäßig damit rechnen, dass seine Nutzungsdaten, einschließlich getätigter Eingaben, von einem KI-System verarbeitet werden, sodass die Verarbeitung insoweit zulässig ist. Dagegen wird der Betroffene auch in diesen Konstellationen wohl nicht erwarten müssen, dass Daten auch zur Weiterentwicklung genutzt werden; im Falle einer solchen – potenziell dauerhaften – Nutzung seiner Daten ohne direkte Einsichtsmöglichkeit überwiegt dessen Interesse an der Nichtverarbeitung.[44] Neben fortlaufendem KI-Training wirft auch die Abfrage weiterer Informationen aus dem Internet Probleme auf: Zwar ist anerkannt, dass von Betroffenen offensichtlich öffentlich zugänglich gemachte Informationen, zB auf eigenen Websites oder in sozialen Netzwerken, einen geringeren Schutzbedarf genießen.[45] Offensichtlich ist die Veröffentlichung jedoch nur bei aktiver Mitwirkung des Betroffenen. Ob die verarbeiteten Daten tatsächlich vom jeweiligen Betroffenen selbst willentlich in die Öffentlichkeit getragen wurden, lässt sich aus Sicht des KI-Nutzers nicht zuverlässig herausfinden. Dem Einsatz solcher KI-Systeme ist damit das Risiko einer rechtswidrigen Datenverarbeitung immanent. Zudem stößt die Rechtsgrundlage an ihre Grenzen, wenn dabei auf Daten Minderjähriger zugegriffen wird (Art. 6 I UAbs. 1 Buchst. f DS-GVO aE). Im Übrigen ist das Ergebnis der Interessenabwägung von zahlreichen Umständen im Einzelfall abhängig, etwa Einsatzzweck, Umfang der Daten, Auswirkungen auf den Betroffenen oder Datensicherheit;[46] auch das Risiko der Erzeugung inhaltlich unrichtiger Daten mag in diese Bewertung einfließen. Letztlich verbleibt – was im Einzelfall zu beurteilen sein wird – in vielen Einsatzszenarien einzig die Interessenabwägung als praxistaugliche Rechtsgrundlage für den Einsatz von KI-Systemen,[47] wenngleich selbst ihr Anwendungsbereich im Falle der Weiterentwicklung oder des Internetzugriffs begrenzt ist.

b) Verarbeitung sensibler Daten

Herausforderungen birgt die Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art. 9 I DS-GVO („sensibler Daten"). Hierbei handelt es sich u.a. um Informationen über politische Meinung, religiöse Überzeugung, sexuelle Orientierung, um biometrische Daten und Gesundheitsdaten. Da viele Daten

mittelbar sensible Rückschlüsse zulassen, vertritt die Literatur nahezu[48] durchweg eine teleologische Reduktion des Art. 9 I DS-GVO.[49] Der EuGH versteht den Begriff jedoch weit und will auch mittelbar-sensible Daten erfassen.[50]

Eine dem „berechtigten Interesse“ äquivalente Rechtsgrundlage existiert für die Verarbeitung sensibler Daten nicht.[51] Im Einzelfall kann es sicherlich erforderlich sein, KI im Beschäftigungsverhältnis (Art. 9 II Buchst. b DS-GVO) einzusetzen, etwa wenn es um die effiziente Erfüllung arbeitsrechtlicher Pflichten geht oder der KI-Einsatz in einer Betriebsvereinbarung vorgesehen ist. Dabei ist zu beachten, dass es sich idR um Hochrisiko-KI[52] handeln dürfte. Darüber hinaus kann der Einsatz von KI im Gesundheitswesen (Art. 9 II Buchst. c, h, i DS-GVO) und bei der Verfolgung bestimmter öffentlicher Interessen (Art. 9 II Buchst. g, j DS-GVO) rechtmäßig sein. Auch der KI-Einsatz im Bereich der Rechtsberatung – gerade bei stark automatisierbaren Verfahren, etwa bei Geltendmachung von Fluggastrechten oder von Schadensersatz nach Datenpannen – mag zulässig sein (Art. 9 II Buchst. f DS-GVO).

Liegt ein solcher Fall nicht vor, kann sich eine Zulässigkeit aus Art. 9 II Buchst. e DS-GVO ergeben: Nach dieser Vorschrift ist eine Verarbeitung sensibler Daten, die der Betroffene „offensichtlich öffentlich gemacht hat“, zulässig. Greift ein KI-System auf das Internet zu, kommt die Vorschrift als Rechtsgrundlage für die Verarbeitung sensibler Daten prinzipiell in Betracht,[53] allerdings kann das einsetzende Unternehmen – wie bereits erläutert – nicht beurteilen, ob Informationen, auf die zugegriffen wurde, durch den Betroffenen veröffentlicht wurden. Werden hingegen Daten nicht öffentlich gemacht, sondern diese Informationen dem Verantwortlichen vom Betroffenen mitgeteilt (Übersendung eigener Daten an den KI-Nutzer), so wäre daran zu denken, Art. 9 II Buchst. e DS-GVO argumentum a maiore ad minus auch auf den Fall anzuwenden, dass der Betroffene gerade nicht die Öffentlichkeit, sondern lediglich einen (kleinen) Teil dieser – das KI-einsetzende Unternehmen – adressiert,[54] sodass die Verarbeitung rechtmäßig ist.

c) Verarbeitung aufgedrängter Daten

Wird eine KI betrieben und anderen Beteiligten zur Nutzung überlassen, zB bei Einsatz eines KI-gestützten Chatbots auf der Unternehmenswebseite, stellt sich darüber hinaus auch das Problem aufgedrängter Daten. Denn der (vermeintlich) Verantwortliche kann nicht absehen, welche personenbezogenen Daten – uU sensible Daten völlig Unbeteiligter – von Dritten dort eingegeben werden. Hier liegt nah, jedenfalls soweit es sich um Informationen ohne Bezug zum Einsatzszenario handelt, im Wege teleologischer Reduktion eine Verarbeitung iSd Art. 2 I, Art. 4 Nr. 2 DS-GVO abzulehnen oder – bei Negation eines voluntativen Elements des Verarbeitungsbegriffs – keine die Verantwortlichkeit iSd Art. 4 Nr. 7 DS-GVO begründende „Entscheidung“ über Zwecke und Mittel der Verarbeitung anzunehmen.[55] Eine Rechtsgrundlage wird daher nicht benötigt, es sei denn, das Unternehmen schwingt sich zum Verantwortlichen auf, indem es die aufgedrängten Daten billigend zur Kenntnis nimmt und nicht unverzüglich löscht (i.E. also über Zwecke bestimmt).

2. Automatisierte Entscheidungen („Profiling“)

Eine weitere Hürde stellt Art. 22 I DS-GVO dar. Nach dieser Vorschrift ist es verboten, eine betroffene Person einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zu unterwerfen, sofern diese Entscheidung rechtliche Wirkung entfaltet oder den Betroffenen in ähnlicher Weise erheblich beeinträchtigt. Der EuGH hat zum Bonitätsscoring durch die Schufa entschieden, dass nicht erst die spätere Entscheidung, sondern bereits die automatisierte Erstellung der Entscheidungsgrundlage (der sog. „Schufa-Score“) dem Anwendungsbereich der Vorschrift unterfallen kann, sofern diese eine erhebliche Relevanz für die spätere Entscheidung unter menschlicher Mitwirkung hat.[56] Einzelne Aufsichtsbehörden sehen großflächige Auswirkungen auf den Einsatz von KI-Systemen: Werden diese eingesetzt, um computergenerierte Vorschläge zu entwerfen, die eine Entscheidungsgrundlage bilden sollen (zB im Bewerbungsverfahren), kann der Anwendungsbereich des Art.

22 DS-GVO eröffnet sein.[57] Die Anwendung der Norm ließe sich dann nur vermeiden, wenn autonome KI-Einschätzungen in jedem Einzelfall durch eine natürliche Person überprüft werden, was Detailkenntnis von der Funktionsweise der KI sowie Möglichkeit der Übersteuerung voraussetzt.[58] Aufsichtsbehörden fordern bei KI-gestützten Entscheidungen, dass ein Freigabeverfahren zu implementieren ist und die menschliche Entscheidung revisionssicher dokumentiert wird.[59] Zudem soll nicht nur die Dateneingabe hinsichtlich sensibler Daten, sondern auch der Output des genutzten KI-Systems regelmäßig auf das Vorhandensein sensibler Daten überprüft werden.[60]

Im Anwendungsbereich des Art. 22 I DS-GVO kommt der KI-Einsatz für (vorbereitende) Entscheidungen nur in den Grenzen des Art. 22 II DS-GVO in Betracht, dh die betroffene Person muss entweder ausdrücklich in den KI-Einsatz eingewilligt haben (Art. 22 II Buchst. c DS-GVO) oder die Entscheidung muss für Abschluss oder Erfüllung eines Vertrags zwischen Betroffenem und Verantwortlichem erforderlich sein (Art. 22 II Buchst. a DS-GVO). Sowohl Anwendungsbereich als auch Reichweite der letztgenannten Ausnahme sind jedoch höchst umstritten.[61] Selbst wenn eine automatisierte Entscheidung unter einen der vorgenannten Ausnahmetatbestände fällt, hat das Unternehmen zusätzliche Maßnahmen zu ergreifen, die u.a. vorsehen, dass der Betroffene die Kontrolle der Entscheidung durch den Verantwortlichen erwirken und die getroffene Entscheidung anfechten kann (Art. 22 III DS-GVO).

Schließlich sind KI-Entscheidungen erlaubt, soweit diese nach unionalem oder mitgliedstaatlichem Recht zulässig sind (Art. 22 II Buchst. b DS-GVO). Dies umfasst ggf. auch die Verarbeitung sensibler Daten.[62] Gerade ein solcher Fall kann jedoch nach Geltung der KI-Verordnung gegeben sein.[63]

3. Betroffenenrechte

Die größte Friktion im Spannungsfeld zwischen KI und Datenschutz offenbart sich aber bei den in Kap. 3 der DS-GVO geregelten Betroffenenrechten.

a) Information der Betroffenen

Werden Daten verarbeitet, so ist der Betroffene grundsätzlich über die Datenverarbeitung gem. Art. 13 f. DS-GVO – etwa über Identität des Verantwortlichen, Zwecke und Rechtsgrundlagen der Verarbeitung, Dauer der Speicherung – zu informieren.

Im Fall der durch Art. 13 DS-GVO geregelten Datenerhebung beim Betroffenen kann die Information über die Verarbeitung mittels des KI-Tools im Rahmen der (in der Praxis ohnehin erfolgenden) Informationen zum Datenschutz erfolgen. Allerdings birgt auch dieser einfache Fall eine KI-spezifische Herausforderung: Nach Art. 13 II Buchst. f DS-GVO sind im Falle einer automatisierten Entscheidungsfindung iSd Art. 22 DS-GVO vom Verantwortlichen „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ zur Verfügung zu stellen. Die Anforderungen an die zu erteilenden Informationen sind umstritten; zumindest wird die allgemeine Funktionsweise des KI-Systems und die Auswirkungen seines Einsatzes so verständlich wie möglich dargestellt werden müssen.[64]

Komplexer wird es, wenn das KI-System genutzt wird, um Informationen über andere Personen zu generieren und/oder im Rahmen des Einsatzes Informationen aus anderen Quellen – seien es andere Unternehmen, Behörden oder dem Internet – abgerufen werden (Dritterhebung). Besteht kein Kontakt zur betroffenen Person, ist die Informationserteilung erschwert. Zudem verfügt der Verantwortliche beim Informationsabruf aus öffentlichen Quellen wie dem Internet selten über die exakte Herkunft der der Datenausgabe zugrundeliegenden Informationen, was eine vollständige Information hierüber (Art. 14 II Buchst. f DS-GVO) erschwert. Zudem gilt auch hier die Pflicht zur verständlichen Erklärung der Funktionsweise des KI-Systems.[65]

Zwar bestimmt Art. 11 I DS-GVO, dass ein Verantwortlicher nicht zur bloßen Einhaltung datenschutzrechtlicher Vorschriften zusätzliche Informationen einholen muss, um die betroffene Person zu identifizieren. Dies disponiert jedoch nicht von der Einhaltung der Art. 13 und 14 DS-GVO.[66] Lediglich im Falle der Dritterhebung kennt das Gesetz eine für den KI-Einsatz relevante Ausnahme: Nach Art. 14 V Buchst. b Hs. 1 DS-GVO kann die Information unterbleiben, wenn ihre Erteilung sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. Je nach eingesetztem KI-System wird das Unternehmen jedoch nicht in der Lage sein, alle Personen, deren Daten verarbeitet werden, zu kontaktieren. Dies gilt umso eher, wenn das KI-System Zugriff auf große Datenbestände nehmen kann und/oder sich in den Ausgabedaten keine Daten widerspiegeln, die eine Zuordnung zu den (vermeintlich) betroffenen Personen oder jedenfalls nicht zu all jenen, deren Daten verarbeitet wurden, zulassen. Selbst wenn der Verantwortliche theoretisch über Kontaktmöglichkeiten verfügte, dürfte es häufig unmöglich sein, herauszufinden, wen er informieren müsste. Im Rahmen der zweiten Tatbestandsalternative – Informationserteilung wäre unverhältnismäßig – sind die Informationsinteressen der betroffenen Personen mit dem Aufwand der Information abzuwägen. Ein unverhältnismäßiger Mitteilungsaufwand kann sich auch daraus ergeben, dass von einer Datenerhebung zahlreiche Personen betroffen sind, deren Interessen hierdurch jeweils nur in geringfügigem Ausmaß beeinträchtigt werden.[67] Dies dürfte etwa dann der Fall sein, wenn das KI-System die genutzten personenbezogenen Daten allein öffentlich zugänglichen Quellen entnimmt.[68] Zum Teil wird pauschal vertreten, im Falle öffentlich zugänglicher Informationen trete das Informationsinteresse der Betroffenen zurück.[69] Allerdings kann eine (verhältnismäßige) Pflicht zur Information bestehen, sofern personenbezogene Daten ausgegeben werden, insbesondere dann, wenn das KI-System durch eine entsprechende Eingabe oder Konfiguration dazu veranlasst wurde, gerade über diese Person(en) Daten zu verarbeiten. Insoweit „klassische“ Einsatzszenarien sind die Bewertung einer Person bzw. ihrer Leistungen, die Analyse oder Zusammenfassung von Lebensläufen oder ähnlicher Dokumente oder die Personenrecherche.

b) Recht auf Auskunft

Jeder Betroffene hat ein Recht auf Auskunft und Datenkopie (Art. 15 I und III DS-GVO). Dabei kann, ähnlich wie bei der Information, auch eine verständliche Erklärung des KI-Systems geschuldet sein (Art. 15 I Buchst. h DS-GVO). Die Vorschrift zum Auskunftsrecht enthält, anders als Art. 14 DS-GVO, keine spezifischen Ausnahmen. Allerdings erklärt Art. 11 II 2 DS-GVO die Art. 15–20 für unanwendbar, wenn der Verantwortliche nachweisen kann, den Betroffenen nicht identifizieren zu können. Hieraus folgt im Grundsatz, dass sich die Pflicht zur Auskunft auf eine Pflicht zur Unterrichtung der auskunftsbegehrenden Person reduziert.[70] Dies wird häufig der Fall sein, wenn sich der Personenbezug nicht konkret in Ein- oder Ausgabedaten widerspiegelt.

c) Datenrichtigkeit

Eine weitere Herausforderung stellt das Gebot der Datenrichtigkeit dar, wonach unrichtige Daten unverzüglich gelöscht oder berichtigt werden müssen (Art. 5 I Buchst. d DS-GVO). Damit korrespondiert auch der Berichtigungsanspruch des Betroffenen (Art. 16 DS-GVO). Funktionierende KI-Systeme erwecken bei ihren Nutzern den Eindruck der inhaltlichen Richtigkeit von Ausgaben. Da bspw. Large Language Models Texte auf Grundlagen reiner Probabilistik ausgeben, besteht dennoch ein – je nach Einsatz/Training unterschiedliches – Risiko der Ausgabe inhaltlich unrichtiger personenbezogener Daten, indem etwa wahrscheinliche, aber unzutreffende Tatsachen erfunden werden oder fehlerhafte Annahmen den von der KI vorgenommenen Bewertungen zugrundegelegt werden.[71] Dieses „Halluzinieren“ von KI ist (zumindest bei generativen Modellen) als statistisches Nebenprodukt unvermeidlich. Eine Ausnahme kennt die DS-GVO nicht, weshalb der Einsatz diverser KI-Systeme in prinzipiellem Widerspruch zum Gebot der Datenrichtigkeit steht.[72]

4. Drittlandtransfers

Zahlreiche KI-Anbieter sind nicht innerhalb der Europäischen Union belegen, sondern erbringen ihre Dienste aus den USA. In diesem Fall sind die Anforderungen der Art. 44 ff. DS-GVO einzuhalten. Maßgeblich ist dann, ob ein Angemessenheitsbeschluss iSd Art. 45 DS-GVO vorliegt; ansonsten ist der Abschluss von Standarddatenschutzklauseln[73] zu empfehlen. Für die USA hat die Europäische Kommission im Juli 2023 die Angemessenheit des US-Datenschutzniveaus festgestellt.[74] Dieser Angemessenheitsbeschluss ist allerdings auf nach dem Data Privacy Framework zertifizierte Unternehmen beschränkt.[75]

IV. Datenschutzrechtliche Aspekte der KI-Verordnung

Das im Juli 2024 verkündete und am 1.8.2024 in Kraft getretene „Gesetz über künstliche Intelligenz" (KI-Verordnung – KI-VO) regelt im Wesentlichen das Inverkehrbringen und den Betrieb von KI-Systemen sowie das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck.

1. Anwendungsbereich und Adressaten

Die KI-VO kennt sechs Akteure: den Anbieter, Produkthersteller, Betreiber, Bevollmächtigten, Einführer oder Händler von KI-Systemen.[76] Dabei weist der Begriff des Anbieters hohe Schnittmengen mit dem Betreiber und dem Hersteller auf, da auch das Entwickeln und Inverkehrbringen eines KI-Systems sowie die Inbetriebnahme eines KI-Systems unter eigenem Namen bereits zur Einstufung als „Anbieter" iSd Art. 3 Nr. 3 KI-VO führt. Für eine Einstufung als „Betreiber", dh den bloßen Verwender eines KI-Systems (Art. 3 Nr. 4 KI-VO), bleibt wenig Raum. Zu denken ist etwa an rein unternehmensintern genutzte KI, welche gegebenenfalls per API auf ein fremdes KI-System zugreift. Zu beachten ist jedoch, dass eine wesentliche Veränderung eines (fremd) angebotenen KI-Systems durch den Betreiber diesen selbst zum Anbieter erstarken lassen kann.[77] Schließlich werden natürliche Personen, die KI-Systeme nicht selbst anbieten, aber diese „betreiben", von den Pflichten der KI-VO freigestellt, sofern sie das KI-System im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwenden.[78] Insoweit besteht weitgehend Gleichlauf mit der Haushaltsausnahme der DS-GVO.[79]

Dreh- und Angelpunkt aller Akteursdefinitionen ist jedoch das „KI-System". Der Begriff der Künstlichen Intelligenz ist nicht neu, sondern geht auf das Jahr 1955 zurück.[80] In seiner heutigen Verwendung ist der Begriff ebenso schillernd wie schwammig, was sich nicht zuletzt in den divergierenden Ergebnissen ähnlicher Studien zeigt: So gaben 20 % der deutschen Unternehmen im Jahr 2019 an, bereits vor 2010 KI produktiv eingesetzt zu haben[81] – in einer anderen Studie gaben hingegen nur 14 % der deutschen Unternehmen an, im Jahr 2022 KI eingesetzt zu haben.[82] Die meisten KI-Entwicklungen, die von Unternehmen eingesetzt werden, basieren auf Machine Learning – die Einsatzmöglichkeiten von „KI" sind allerdings mannigfaltig,[83] weshalb KI, ebenso wie alle anderen Algorithmen, eher als technischer Zwischenschritt denn als Produkt begriffen werden sollte.

Nach Art. 3 Nr. 1 KI-VO ist ein „KI-System" ein maschinengestütztes System, das für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, welche physische oder virtuelle Umgebungen beeinflussen können. Die Definition ist weit und geeignet, beinahe jegliche Software zu erfassen.[84] In diesem Sinne ist KI auch der Regulierung mittels des technologieneutralen Ansatzes des Datenschutzrechts zugänglich und bedürfte keiner Sondervorschriften, wenngleich sich Besonderheiten im Schnittbereich von KI-VO und DS-GVO ergeben.

2. Datenschutzbezogene Pflichten aus der KI-Verordnung

Nach Art. 2 VII 2 KI-VO berühre die Verordnung die DS-GVO grundsätzlich nicht – eine These, die sich so sicherlich nicht halten lässt und noch in den Erwägungsgründen widerlegt wird.[85] Vielfach verweist die KI-VO auf die DS-GVO und ergänzt diese. Eine vollständige Darstellung der Pflichten der Adressaten kann an dieser Stelle nicht erfolgen. Gleichwohl soll überblicksartig auf spezifische Pflichten mit Datenschutzbezug eingegangen werden.

a) Abgestuftes Pflichtenprogramm

Begrenzt wird der weite Anwendungsbereich der KI-Verordnung durch ein risikoabhängiges Pflichtenprogramm, wonach bestimmte KI-Anwendungen verboten sind[86] und Hochrisiko-KI-Systeme sowie general purpose AI[87] – durch Kap. 3 bzw. 5 der KI-VO einem ausführlichen Pflichtenprogramm unterworfen werden. Beim Anbieten oder Betreiben „normaler" KI-Systeme sind lediglich die Transparenzpflichten des Art. 50 KI-VO zu beachten.

b) Rechtsgrundlagen und Datenrichtigkeit

Die ausführlichsten datenschutzbezogenen Pflichten treffen die Anbieter von Hochrisiko-KI-Systemen iSd Art. 6 KI-VO. Dabei handelt es sich überwiegend um KI-Systeme, die biometrische Daten verarbeiten, in kritischen Infrastrukturen oder im Bildungssektor eingesetzt werden, der Auswahl, Beurteilung oder Entscheidung im Beschäftigungskontext dienen, über die Zugänglichkeit und Inanspruchnahme grundlegender Dienste und Leistungen entscheiden oder in den Bereichen Strafverfolgung, Migration, Rechtspflege und Wahlen eingesetzt werden.[88] Nicht zuletzt dadurch, dass eine Vielzahl heutiger Software den Begriff des „KI-Systems" erfüllen wird, dürften zahlreiche im Rahmen von eLearning, Arbeitnehmerauswahl und -leistungsmessung, Kreditvergabe und Preisbildungsverfahren eingesetzter Tools als Hochrisiko-KI einzustufen sein.

Beim Training von Hochrisiko-KI sind u.a. die Vorschriften über Data Governance gem. Art. 10 KI-VO zu beachten, welche vor allem die Qualität beim Einsatz des KI-Systems sicherstellen soll. Der enge Zusammenhang mit dem Gebot der Datenrichtigkeit[89] kommt etwa in Abs. 2 zum Ausdruck. Zur Qualitätssicherung sollen Trainings-, Validierungs- und Testdatensätze – die auch personenbezogene Daten erhalten können – verwendet werden. In diesen Fällen wirkt, soweit die Nutzung von personenbezogenen Daten für die Data Governance erforderlich ist, Art. 10 I KI-VO als rechtliche Pflicht iSd Art. 6 I UAbs. 1 Buchst. c DS-GVO und damit die Datenverarbeitung legitimierend. Nach Art. 10 V 1 KI-VO dürfen, soweit dies für die Erkennung und Korrektur von Verzerrungen erforderlich ist und solange dabei die in Art. 10 V 2 Buchst. a bis f KI-VO genannten Kriterien eingehalten werden, auch sensible Daten verwendet werden. Die Vorschrift bildet damit eine unionsrechtliche Vorschrift, die spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen Betroffener vorsieht iSd Art. 9 II Buchst. g DS-GVO. Das von Art. 9 II Buchst. g DS-GVO geforderte „erhebliche öffentliche Interesse" ist hierbei der Schutz Betroffener vor fehlerbehaftetem Einsatz von Hochrisiko-KI.

Zudem sieht Art. 12 KI-VO vor, dass Ereignisse beim Einsatz von Hochrisiko-KI-Systemen protokolliert werden. Dies umfasst u.a. Eingabedaten, welche personenbezogen sein können, aber auch die Identität der die menschliche Aufsicht über das KI-System führenden Personen.[90] Hierbei handelt es sich ebenfalls um eine Rechtsgrundlage iSd Art. 6 I UAbs. 1 Buchst. c und – falls die Eingabedaten als sensible Daten zu qualifizieren sind – iSd Art. 9 II Buchst. g DS-GVO.

Schließlich müssen Hochrisiko-KI-Systeme den in Art. 15 KI-VO geregelten IT-Sicherheitsanforderungen genügen. Die Vorschrift, deren Regelungsgehalt eng mit den in Art. 32 DS-GVO geregelten Datensicherheitsanforderungen verknüpft ist, soll nicht nur Störungen verhindern, sondern auch Fehlern und Unstimmigkeiten vorbeugen. Vielfach dürfte diese gesetzliche Pflicht die Verarbeitung personenbezogener Daten nach Art. 6 I UAbs. 1 Buchst. c DS-GVO erforderlich machen.

c) Betroffenenrechte

Wird KI in direkter Interaktion mit natürlichen Personen eingesetzt, so ist der Anbieter – unabhängig vom Risikoniveau des KI-Systems – zur Information über den KI-Einsatz verpflichtet (Art. 50 I KI-VO). Betreiber von Emotionserkennungssystemen und Systemen zur biometrischen Kategorisierung sind ebenso zur Information betroffener Personen verpflichtet (Art. 50 III KI-VO). Diese Art. 13 f. DS-GVO flankierende Pflicht gilt ungeachtet der Risikoeinstufung und des Umstands, ob ein direkter Kontakt zum Betroffenen besteht – wenngleich dies bei derartigen KI-Systemen qua natura naheliegt.

Die Vorgaben beim Betrieb von Hochrisiko-KI treten zu den vorstehenden Vorgaben hinzu.[91] So sind Betreiber von Hochrisiko-KI-Systemen in den von Art. 26 VII und XI KI-VO erfassten Fällen verpflichtet, die von der Verwendung dieser Systeme Betroffenen über den Einsatz von Hochrisiko-KI zu informieren. Datenschutzrechtlich bedeutsam ist auch Art. 14 KI-VO, der eine menschliche Aufsicht über Hochrisiko-KI-Systeme fordert. Die Vorschrift sieht u.a. vor, dass natürliche Personen den Betrieb des Systems überwachen, und die Möglichkeit haben, das System nicht zu verwenden, es stillzulegen sowie Ausgaben außer Acht zu lassen und rückgängig zu machen. Dies ähnelt der Empfehlung der Behörden, bei KI-gestützten Entscheidungen ein Freigabeverfahren zu implementieren, wodurch der Anwendungsbereich des Art. 22 I DS-GVO uU nicht eröffnet wird.[92]

d) Folgenabschätzung(en)

Die Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO (DSFA) ist eine Prüfung, die vom Verantwortlichen durchzuführen ist, wenn eine Verarbeitungstätigkeit voraussichtlich zu einem hohen Risiko für Rechte und Freiheiten natürlicher Personen führt. Dabei soll eine DSFA vor allem dann geboten sein, wenn eine systematische und umfassende Bewertung persönlicher Aspekte erfolgt, welche den Anforderungen des Art. 22 DS-GVO unterliegt.[93] Datenschutzaufsichtsbehörden gehen davon aus, dass eine DSFA beim KI-Einsatz regelmäßig erforderlich ist.[94] Betreiber eines Hochrisiko-KI-Systems sollen nach Art. 26 IX KI-VO die bereitgestellten Informationen, dh die gem. Art. 13 KI-VO zur Verfügung gestellte Betriebsanleitung verwenden, um die DSFA durchzuführen.

Zudem soll vor Inbetriebnahme bestimmter Hochrisiko-KI-Systeme eine Grundrechte-Folgenabschätzung durchgeführt werden, in deren Rahmen die Auswirkungen des Systems auf Grundrechte evaluiert werden (Art. 27 KI-VO). Dabei ist zu beachten, dass die hiermit verbundenen Pflichten ganz oder teilweise entfallen können, sofern und soweit diese bereits bei der Durchführung einer DSFA erfüllt wurden.[95]

3. Geltungsbeginn

Grundsätzlich gilt die KI-VO gem. Art. 113 nach 24 Monaten ab Inkrafttreten – also ab dem 1.8.2026. In Abhängigkeit von der eigenen Rolle als KI-Akteur und der Art der eingesetzten KI-Systeme gelten einige Pflichten bereits nach zwölf Monaten. Einzig das Verbot bestimmter KI-Praktiken (Art. 5 KI-VO) findet bereits nach sechs Monaten, dh ab dem 1.2.2025, Anwendung. Für KI-Nutzer ist essenziell, festzustellen, ob diese als Anbieter oder Betreiber tätig sind, und zeitnah zu prüfen, ob es sich bei den eingesetzten KI-Systemen um „normale“ KI, Hochrisiko-KI oder gar um verbotene Anwendungen handelt, da hiervon die zu treffenden Maßnahmen und der Zeitplan wesentlich abhängen.

V. Fazit

Der Einsatz von KI-Systemen wirft zahlreiche datenschutzrechtliche Probleme auf. Teils sind Grundsatzfragen ungeklärt: KI-Nutzer sind gut beraten, eine KI-Strategie zu entwickeln, welche Fragen nach der Personenbeziehbarkeit von Daten, der Risikoeinstufung ihrer Systeme und der Verteilung datenschutz- und KI-rechtlicher Rollen adressiert. Sodann bietet das Datenschutzrecht hinreichend tragfähige Rechtsgrundlagen. Die neue KI-VO mit ihrem weiten Anwendungsbereich liefert dabei (eher unfreiwillig) wertvolles Argumentationsmaterial. Offensichtlich wird das Spannungsverhältnis im Bereich der Betroffenenrechte, welche durch die KI-VO ergänzt werden. Grundlegende Veränderungen des datenschutzrechtlichen Regelungsrahmens, etwa

beim Grundsatz der Datenrichtigkeit, bringt die KI-VO nicht. Mitunter birgt das Geflecht von Datenschutz- und KI-Regulierung zwar Synergien, die drohende Sanktion im Falle von Verstößen gegen eine der beiden Verordnungen aber zugleich die Gefahr eines Vabanquespiels. Auch hier sind Lösungen möglich, setzen aber einen gewissen „risk appetite“ voraus. KI und Datenschutz können in einigen Anwendungsszenarien vereinbar sein – müssen dafür jedoch in der Compliance holistisch betrachtet und ebenso in der Organisation umgesetzt werden.

* Der Autor ist Inhaber der Professur für Wirtschaftsrecht, insbes. Recht der Digitalisierung, an der FH Aachen, Of Counsel bei PricewaterhouseCoopers und External Expert des Europäischen Datenschutzausschusses.

1 World Economic Forum, The Future of Jobs, Report 2023, S. 6.

2 Derzeit Gegenstand zahlreicher Verfahren, s. allein die Urteile der Oberlandesgerichte, etwa OLG Celle 4.4.2024 – 5 U 31/23, GRUR-RS 2024, 6435; OLG Hamm GRUR 2023, 1791; OLG Frankfurt a. M. NJW-RR 2024, 123 uvm. Allgemein zur datenschutzrechtlichen Verantwortlichkeit und Rechtmäßigkeit des Scraping Mertens/Meyer K & R 2023, 563; zu datenschutzrechtlichen Aspekten von Scraping zwecks KI-Training Dieker ZD 2024, 132; Paal ZfDR 2024, 129 (146 ff.).

3 DSK, Regulierung von KI: DSK fordert klare Verantwortlichkeit für Hersteller und Betreiber, 29.11.2023.

4 Der weit verstandene Verarbeitungsbegriff (Art. 4 Nr. 2 DS-GVO) erfasst jeden Umgang mit personenbezogenen Daten, Simitis/Hornung/Spiecker gen. Döhmann/Roßnagel Datenschutzrecht, 2. Aufl. 2024, DS-GVO Art. 4 Nr. 2 Rn. 10 f.

5 Vgl. Art. 1 I DS-GVO.

6 Art. 4 Nr. 1 DS-GVO.

7 Vgl. auch das in Art. 16 DS-GVO geregelte Recht auf Berichtigung.

8 Taeger/Gabel/Arning/Rothkegel DSVGO-BDSG-TTDSG, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 24 ff.; Simitis/Hornung/Spiecker gen. Döhmann/Karg, 2. Aufl. 2024, DS-GVO Art. 4 Nr. 1 Rn. 54.

9 Statt vieler Kühling/Buchner/Klar/Kühling DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 1 Rn. 25 ff.

10 EuGH ECLI:EU:C:2016:791 = BeckRS 2016, 82523 – Plöckl (C-24/15).

11 EuG ECLI:EU:T:2023:219 = ZD 2023, 399 mAnm Baumgartner – SRB/EDSB (T-557/20), beim EuGH als Rs. C-413/23 anhängig.

12 Zu technischen Grundlagen von Large Language Models Pesch/Böhme MMR 2023, 917 (918 f.).

13 Beachte aber zB Nasr et al., arXiv:2311.17035, die in der Lage waren, personenbezogene Daten aus ChatGPT zu extrahieren. Gleichwohl muss bezweifelt werden, dass dies unter Einsatz von Mitteln erfolgte, die „nach allgemeinem Ermessen wahrscheinlich genutzt werden“ (Erwgr. 26 S. 3 der DS-GVO) und somit zu einem Personenbezug führen.

14 Paal/Pauly/Martini DS-GVO/BDSG, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 2.

15

Die hM spricht von einer „Privilegierung", etwa Taeger/Gabel/Gabel/Lutz , 4. Aufl. 2022, DS-GVO Art. 28 Rn. 8 ff.; Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 28 Rn. 16 ff.; Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 8a.

16 Vgl. Art. 4 Nr. 8, Art. 28 III Buchst. a DS-GVO.

17 Art. 28 X DS-GVO.

18 Vgl. Art. 28 S. 2 III Buchst. a DS-GVO.

19 Petersen PinG 2023, 122.

20 LfDI BW, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz", 2024, S. 10.

21 EDPB, Guidelines 7/2020, Version 2.1, S. 12.

22 In diese Richtung auch Ashkar ZD 2023, 523 (525); LfDI BW, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz", 2024, S. 9, 11.

23 Grundlegend EuGH ECLI:EU:C:2018:388 = EuZW 2018, 534 – Wirtschaftsakademie Schleswig-Holstein (C-210/16); s. hierzu auch Golland K & R 2018, 433.

24 Erstmals EuGH ECLI:EU:C:2018:551 Rn. 58, 66, 69 = EuZW 2018, 897 – Jehovan todistajat (C-25/17), zuletzt bestätigt durch EuGH ECLI:EU:C:2024:214 = ZD 2024, 328 – IAB Europe (C-604/22).

25 EuGH ECLI:EU:C:2023:949 Rn. 40 = ZD 2024, 209 – Nacionalinis visuomenės sveikatos centras (C-683/21); EuGH ECLI:EU:C:2024:214 Rn. 57 = ZD 2024, 328 – IAB Europe.

26 So bietet etwa OpenAI den Nutzern von ChatGPT einen Auftragsverarbeitungsvertrag an.

27 Der Vertragsabschluss wirkt nicht konstitutiv für die Auftragsverarbeitung, Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 28 Rn. 61.

28 Unten III.1 und .3.

29 Vgl. Art. 26 III DS-GVO.

30 Golland ZD 2020, 397 (400).

31 ZT wurde vertreten, Art. 9 II DS-GVO sei lex specialis zu Art. 6 I DS-GVO. Dieser Ansicht hat der EuGH jedoch eine Absage erteilt, s. EuGH EuZW 2024, 270 Rn. 78 f.

32

Zur Rechtmäßigkeit des KI-Einsatzes im Beschäftigungskontext Hersemeyer/Ludolph InTeR 2024, 55 (57 ff.); Witteler/Moll NZA 2023, 327 (328 ff.).

33 Art. 4 Nr. 11 DS-GVO.

34 Explizit zum KI-Einsatz LfDI BW, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“, S. 19; allgemein zur Möglichkeit der Einwilligung in Beschäftigungsverhältnissen Taeger/Gabel/Zöll, 4. Aufl. 2022, BDSG § 26 Rn. 77 f.

35 Art. 7 III 1 DS-GVO.

36 LfDI BW, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“, 2024, S. 12; Keber/Maslewski RDV 2023, 274 (277).

37 Hessel/Dillschneider RDi 2023, 458 (460); Keber/Maslewski RDV 2023, 274 (277 f.).

38 Ausführlich und mwN: Kühling/Buchner/Buchner/Petri, 4. Aufl. 2024, DS-GVO Art. 6 Rn. 38 ff.; explizit zum KI-Einsatz LfDI BW, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ S. 13.

39 EDPB, Guidelines 2/2019 Version 2.0, S. 9.

40 EuGH ECLI:EU:C:2023:537 Rn. 97 ff. = EuZW 2023, 950 mAnm Wünschelbaum = MMR 2023, 669 mAnm Golland – Meta Platforms u.a. (C-252/21).

41 Hersemeyer/Ludolph InTeR 2024, 55 (58).

42 So auch LfDI BW, Diskussionspapier „Rechtsgrundlagen im Daten-schutz beim Einsatz von Künstlicher Intelligenz“, 2024, S. 16 f.

43 Erwgr. 47 S. 1 DS-GVO.

44 So auch Werkmeister/Laux PinG 2023, 103 (108).

45 Für eine Übertragung der Wertung aus Art. 9 II Buchst. e DS-GVO auch Bernzen K & R 2023, Beil. 1 zu Heft 10/2023, 6 (9 f.); Paal ZfDR 2024, 129 (154).

46 Ein Katalog von Abwägungskriterien findet sich bei Paal ZfDR 2024, 129 (151 ff.).

47 So auch LfDI BW, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“, 2024, S. 18; für das KI-Training anhand öffentlich zugänglicher Daten auch Keber/Maslewski RDV 2023, 274 (277); Paal ZfDR 2024, 129 (153).

48 Beachte aber Simitis/Hornung/Spiecker gen. Döhmann/Petri, 2. Aufl. 2024, DS-GVO Art. 9 Rn. 12.

49

Teils wird ein sensibler Verwendungszusammenhang (zB Taeger/Gabel/Mester, 4. Aufl. 2022, DS-GVO Art. 9 Rn. 6) oder eine auf sensible Daten bezogene Verarbeitungsabsicht (zB Gola/Heckmann/Schulz DS-GVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 13) vorausgesetzt, ausf. und mit Darstellung des Streitstands Britz/Indenhuck/Langerhans ZD 2021, 559.

50 EuGH ECLI:EU:C:2022:601 Rn. 123 ff. = ZD 2022, 611 – Vyriausioji tarnybinės etikos komisija (C-184/20); EuGH ECLI:EU:C:2023:537 Rn. 68 ff. = EuZW 2023, 950 mAnm Wünschelbaum = MMR 2023, 669 mAnm Golland – Meta Platforms u.a.

51 Hieraus folgern Hessel/Dillschneider RDi 2023, 458 (462), eine Verarbeitung sensibler Daten mittels KI sei nicht zulässig.

52 Dazu unten IV.2.b.

53 EDPB, Report of the work undertaken by the ChatGPT Taskforce, 23.5.2024, p. S. 7.

54 Golland MMR 2023, 680 (681).

55 In der Praxis führen beide vorgeschlagenen Lösungsansätze zum selben Ergebnis.

56 EuGH ECLI:EU:C:2023:957 Rn. 48 ff. = EuZW 2024, 75 – SCHUFA Holding (Scoring) (C-634/21). Zuvor noch aA in Bezug auf den KI-Einsatz Ashkar ZD 2023, 523 (530).

57 HmbBfDI, Pressemitteilung „Auswirkungen des Schufa-Urteils auf KI-Anwendungen“, 7.12.2023.

58 AA Kremer CR 2024, 50 (57), der beim KI-Einsatz Art. 22 DS-GVO stets für anwendbar hält.

59 DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 2019, S. 16.

60 DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 2019, S. 18.

61 Einen Überblick gibt Kühling/Buchner/Buchner, 4. Aufl. 2024, DS-GVO Art. 22 Rn. 28 ff.

62 Art. 22 IV DS-GVO.

63 Siehe unten IV.2.b.

64 Die Aufsichtsbehörden verlangen, dass sowohl Ergebnis als auch Prozesse und Zustandekommen einer Erklärung nachvollziehbar sind und erklärbar sein müssen (DSK, Hambacher Erklärung zur Künstlichen Intelligenz, 2019, S. 3). Zum Streitstand Hessel/Dillschneider RDi 2023, 458 (462); ausführlich zum sog. „Recht auf Erklärbarkeit“ Westernhagen/Sánchez Cordero Canela PinG 2023, 112 (117 f.).

65 Art. 14 II Buchst. g DS-GVO.

66 Vgl. Art. 11 II 2 DS-GVO.

67 Kühling/Buchner/Bäcker, 4. Aufl. 2024, DS-GVO Art. 14 Rn. 55.

68 Eine Unverhältnismäßigkeit in diesen Fällen annehmend Franke RDi 2023, 565 (569)).

69 So Werry MMR 2023, 911 (914).

70 Art. 11 II 1: „Kann der Verantwortliche (…) nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich".

71 Zu ChatGPT auch EDPB, Report of the work undertaken by the ChatGPT Taskforce, 23.5.2024, pp. 8 f.

72 So für Large Language Models Werkmeister/Laux PinG 2023, 108 (109 f.); allgemein Chibanguza/Kuß/Steege/Steege/Kuß, Künstliche Intelligenz, Teil 1, § 2 Rn. 66.

73 Kommission Durchführungsbeschluss (EU) 2021/914, ABl. 2021 L 199, 31.

74 Kommission Durchführungsbeschluss (EU) 2023/1795, ABl. 2023 L 231, 118.

75 https://www.dataprivacyframework.gov/s/participant-search.

76 Vgl. Art. 3 Nr. 8 KI-VO.

77 Erwgr. 128 der KI-VO.

78 Art. 3 Nr. 4 Hs. 2 KI-VO.

79 Siehe oben II.2.d.

80 McCarthy et al., A proposal for the Dartmouth summer research project on artificial intelligence, 1955, passim.

81 BMWI, Einsatz von Künstlicher Intelligenz in der Deutschen Wirtschaft. Stand der KI-Nutzung im Jahr 2019, S. 5.

82 DIHK, Digitalisierung tritt auf der Stelle. Digitalisierungsumfrage 2022/2023, S. 11.

83 Einen Überblick über Einsatzszenarien gibt Fraunhofer IMW, Künstliche Intelligenz im Unternehmenskontext, 2019, S. 12 ff.

84 Bereits zum Kommissionsentwurf Bomhard/Merkle RDi 2021, 276 (277 f.).

85 Siehe insbesondere Erwgr. 140 S. 1, wonach die KI-VO eine Rechtsgrundlage für die Verwendung personenbezogener Daten in KI-Reallaboren bilden soll.

86 Art. 5 KI-VO.

87 Nach dem Wortlaut die „KI-Modelle mit allgemeinem Verwendungszweck“, legaldefiniert in Art. 3 Nr. 63 KI-VO.

88 Vgl. Anh. III zu den Hochrisiko-KI-Systemen gem. Art. 6 II KI-VO.

89 Siehe oben III.3.c.

90 Art. 12 III Buchst. c und d KI-VO.

91 Art. 50 VI KI-VO.

92 Oben III.2.

93 Vgl. Art. 35 III Buchst. a DS-GVO; zur Durchführung einer DSFA beim KI-Einsatz Schürmann ZD 2022, 316.

94 DSK, Hambacher Erklärung zur Künstlichen Intelligenz, 2019, S. 4; für das KI-Training mittels öffentlich zugänglicher Daten auch Franke RDi 2023, 565 (570).

95 Art. 27 IV KI-VO.