Moritz W. Rothmund-Burgwall
Research Institute – Digital Human Rights Center

Einsatz von KI als neuartige Datenverarbeitung?

AI Act; KI-System; neuartige Datenverarbeitung. Die Begriffsdefinition zu „KI-System" weist unterschiedliche Merkmale auf, die aus datenschutzrechtlicher Perspektive überaus interessant sind. So besticht der Einsatz von KI-Systemen zur Verarbeitung personenbezogener Daten durch graduell abstufbar autonomes Handeln eines maschinengestützten Systems, kann mit hohen Risiken für betroffene Personen verbunden sein und birgt systemimmanente Intransparenz im Umgang mit Daten. Ob die Verwendung von KI zur Datenverarbeitung mit der automatisierten Verarbeitung iSd DSGVO gleichzusetzen ist, wird im Rahmen dieses Beitrags erörtert.

Einleitung

Sowohl in der Informatik als auch in anderen Bereichen ist die genaue Definition des Begriffs „Künstliche Intelligenz" umstritten.[1] Der Begriff umfasst verschiedene technische Aspekte und ist stark zeitabhängig.[2] Im internationalen sowie unionsrechtlichen Kontext hat man sich auf den Begriff „KI-System" geeinigt. Je nach Anwendungsgebiet geht mit der Verwendung eines KI-Systems die Verarbeitung personenbezogener Daten einher. Dabei können die Daten durch das KI-System nicht einfach nur starr wiedergegeben, sondern in einem bestimmten Kontext mit einer Unmenge an anderen Daten autonom verknüpft werden. Ob dies als rein „automatisierte Verarbeitung" zu werten ist oder mit Blick auf das Charakteristikum der Autonomie darüber hinaus geht, wird im Beitrag beleuchtet.

AI Act – KI-System, GPAI-Modell und GPAI-System

Damit auf Unionsebene eine Kohärenz mit internationalen Instrumenten gewährleistet ist, orientiert sich die **Begriffsdefinition** im **AI Act** stark an der OECD-Variante.[3] Demnach handelt es sich gem Art 3 Z 1 AI Act um *„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".*[4]

Mit anderen Worten handelt es sich bei einem „KI-System" um ein graduell autonom betriebenes, anpassungsfähiges, maschinengestütztes System, das aus Eingaben unterschiedliche Ziele ableitet, die geeignet sind, die Umgebung zu beeinflussen. Die Eigenschaft der **Autonomie** bedingt, dass das KI-System bis zu einem gewissen Grad **unabhängig von menschlichem Zutun** agiert und in der Lage ist, ohne menschliches Eingreifen zu arbeiten.

Das Kriterium der **Anpassungsfähigkeit** bezieht sich auf die Lernfähigkeit des KI-Systems, die es ihm gestattet, sich während der Anwendung weiterzuentwickeln.

Ausgehend von der Tatsache, dass KI-Systeme von Maschinen betrieben werden, sind diese als **„maschinengestützt"** zu bezeichnen.[5]

Die Ableitungsfähigkeit eines KI-Systems geht über eine einfache Datenverarbeitung hinaus.

Das Merkmal der **Ableitungsfähigkeit** umfasst einerseits den Prozess des Erhalts von Ergebnissen, wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, die die physische und virtuelle Umgebung beeinflussen können. Andererseits bezieht sich diese Fähigkeit auch darauf, Modelle oder Algorithmen aus Eingaben oder Daten abzuleiten.[6] Zu Techniken, die das Ableiten beim Aufbau eines KI-Systems ermöglichen, gehören Konzepte für maschinelles Lernen[7] sowie Logik- und wissensgestützte Konzepte.[8] Die Ableitungsfähigkeit eines KI-Systems geht sohin über eine einfache Datenverarbeitung hinaus und ermöglicht Lern-, Schlussfolgerungs- und Modellierungsprozesse.[9]

Um eine **herkömmliche Software** und kein KI-System handelt es sich hingegen, wenn das automatische Ausführen von Operationen ausschließlich auf von natürlichen Personen definierten Regeln beruht.[10]

GPAI-Modell

Im Gegensatz zum Begriff „KI-System" handelt es sich beim „General Purpose AI-Model"[11] (GPAI-Modell) um ein KI-Modell, das auf zwei wesentlichen Merkmalen beruht, nämlich der **allgemeinen Verwendbarkeit** und der Fähigkeit, ein **breites Spektrum unterschiedlicher Aufgaben** kompetent zu erfüllen.[12] Für sich allein genommen stellen KI-Modelle keine KI-Systeme dar, sind aber idR in KI-Systeme integriert und daher wesentliche Komponenten bzw Teil davon.[13] Werden jedoch weitere Komponenten, wie bspw eine Nutzerschnittstelle, einem KI-Modell hinzugefügt, kann es als KI-System qualifiziert werden.[14]

Ein typisches Beispiel für ein GPAI-Modell sind große generative KI-Modelle, die eine flexible Erzeugung von Inhalten (in Form von Text, Audio, Bild oder Video) ermöglichen und sohin ein breites Spektrum unterschiedlicher Aufgaben umfassen können.[15] Zu dieser Kategorie zählen Large Language Models (LLM), die ChatGPT, Google Gemini oder BingAI zugrunde liegen.[16]

Obwohl jedes KI-System auf einem KI-Modell beruhen muss, sieht der AI Act keine spezifischen Regelungen für KI-Modelle vor. Lediglich die Sondergruppe der GPAI-Modelle werden herausgegriffen, zumal sie im Gegensatz zu normalen Modellen in vielen Systemen integriert werden können. Daher ist es sinnvoll, bereits früh

[1] MwN *JRC*, AI Watch. Defining Artificial Intelligence 2.0. Towards an operational definition and taxonomy of artificial intelligence (2021), https://publications.jrc.ec.europa.eu/repository/handle/JRC126426 (Stand aller Links 14. 5. 2024). [2] MwN *Boucher*, Artificial intelligence. How does it work, why does it matter, and what can we do about it? (2020), www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf; *Nilsson*, The quest for artificial intelligence. A history of ideas and achievements (2010). [3] Siehe *OECD*, OECD AI Principles overview, www.oecd.ai/ai-principles. [4] Nachfolgende Verweise auf den AI Act beziehen sich auf die deutschsprachige Version vom 17. 4. 2024, in der zuletzt etwaige Sprach- und Nummerierungsfehler früherer Entwürfe korrigiert wurden, www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf. [5] ErwGr 12 AI Act. [6] Ebd. [7] Hierbei wird aus Daten gelernt, wie bestimmte Ziele erreicht werden können. [8] Hierbei wird aus kodierten Informationen oder symbolischen Darstellungen der zu lösende Aufgabe abgeleitet. [9] ErwGr 12 AI Act. [10] Ebd. [11] Gem Art 3 Z 63 AI Act *„KI-Modell mit allgemeinem Verwendungszweck"*. [12] ErwGr 97 AI Act. [13] Ebd. [14] Ebd. [15] ErwGr 99 AI Act. [16] IW handelt es sich bei LLM um KI-Modelle, die auf Basis einer enormen Datenmenge (Text, Audio, Bild oder Videos) trainiert wurden.

in der Wertschöpfungskette solche Modelle zu regulieren.

GPAI-System

Als ein „General Purpose AI-System“[17] (GPAI-System) wird ein KI-System dann qualifiziert, wenn darin ein **GPAI-Modell integriert** wurde oder ein Teil von diesem ist, wodurch das KI-System in der Lage ist, einer Vielzahl von Zwecken zu dienen.[18] Dabei kann ein GPAI-System sowohl direkt eingesetzt als auch in andere KI-Systeme integriert werden.[19]

Bei ChatGPT, Google Gemini oder BingAI handelt es sich um GPAI-Systeme.

Da ChatGPT, Google Gemini oder BingAI auf GPAI-Modellen beruhen und über weitere Komponenten, wie insb einer Nutzerschnittstelle, verfügen, handelt es sich bei diesen um GPAI-Systeme. Durch den Einsatz eines sog Transformer-Modells bzw neuronalen Netzes, welches aus mehreren Schichten besteht, ist das KI-System in der Lage, neue Inhalte zu generieren. Die Algorithmen errechnen beim Training die statistische Häufigkeit der Aufeinanderfolge von zB Worten und „erraten“ letztendlich bei der Beantwortung von Fragen oder Generierung von Text, was die nächste statistisch wahrscheinlichste Wortfolge im spezifischen Kontext ist.

Datenschutzrechtliche Einordnung des Begriffs „KI-System“

Werden personenbezogene Daten im Rahmen der Entwicklung bzw Nutzung eines KI-Systems verarbeitet, muss diese „Verarbeitung“ aus datenschutzrechtlicher Perspektive beurteilt werden.

Verarbeitung iSd DSGVO

Unter dem Begriff der **„Verarbeitung“** subsumiert man jeglichen Vorgang, der mit oder ohne Hilfe automatisierter Verfahren ausgeführt wird und im Kontext mit personenbezogenen Daten steht.[20] Sowohl die ganz als auch die bloß teilweise automatisierte Verarbeitung unterliegt dem sachlichen Anwendungsbereich der DSGVO.[21] Von einer „teilweise automatisierten Verarbeitung“ spricht man, wenn bereits ein einzelner Datenverarbeitungsvorgang auf einem elektronischen Automatismus beruht.[22]

Werden sämtliche Verarbeitungsschritte *„ohne menschlich-manuelle Interaktion (etwa Tastatureingaben) programmgesteuert bzw elektronisch vorgenommen“*,[23] liegt eine **automatisierte Verarbeitung** vor. Charakteristisch für das Vorliegen einer automatisierten Verarbeitung soll die *„erleichterte Zugänglichkeit und Auswertbarkeit“* von personenbezogenen Daten sein.[24] Unter dem Begriff der automatisierten Verarbeitung kann sohin der Einsatz einer herkömmlichen Software subsumiert werden, zumal hierbei je nach Ausgestaltung Operationen ohne menschlich-manuelle Interaktion programmgesteuert vorgenommen werden können, wobei das automatische Ausführen der Operationen ausschließlich auf von natürlichen Personen festgelegten (und mehr oder weniger vorhersehbaren und nachvollziehbaren) Regeln beruht.

Autonome, risikobehaftete und intransparente Verarbeitung – KI-System

Folgt man dem Verständnis zum Begriff „KI-System“ iSd AI Act, geht der Einsatz von KI-Systemen zur Verarbeitung personenbezogener Daten idR weit über die automatisierte Verarbeitung hinaus. Schließlich heben sich KI-Systeme gerade aufgrund von Kriterien wie autonomer Betrieb, Ableitungsfähigkeit, Möglichkeit der Anpassungsfähigkeit und Beeinflussung der Umgebung von „normalen“ IT-Systemen ab.[25] In Anlehnung an Art 3 Z 1 AI Act ist die automatisierte Verarbeitung als Teil des „maschinengestützten Systems“ zwar der technisch bedingte Ausgangspunkt eines KI-Systems. Dieses muss jedoch darauf aufbauend graduell autonom handeln, kann anpassungsfähig sein und mittels seiner Ergebnisse sein Umfeld beeinflussen.

Durch die beim autonomen Verarbeiten fortlaufende Verknüpfung von Daten entsteht der durch den Einsatz von KI beabsichtigte Mehrwert.

Datenschutzrechtlich steckt dahingehend in dem autonomen Handeln bzw Verarbeiten von Daten das **wesentliche Unterscheidungsmerkmal** zur rein automatisierten Verarbeitung. Es kommt nämlich durch das autonome Verarbeiten fortlaufend zur Verknüpfung diverser Daten, woraus ein informationeller Mehrwert entstehen kann, der durch den Einsatz von KI geradezu beabsichtigt ist. So sollen bspw Muster oder Anomalien durch die Verwendung von KI erkannt werden, was zuvor mittels starrer automatisierter Verarbeitung mangels Anpassungs- und Lernfähigkeit der Systeme nur sehr beschränkt möglich war.

Anzumerken ist auch die **datenschutzrechtliche Verantwortlichkeit** für die autonome Datenverarbeitung. Entschließt sich der Betreiber,[26] ein KI-System entsprechend der Zweckbestimmung in eigener Verantwortung zu verwenden, so kann dieser als Verantwortlicher für die Verarbeitung all jener personenbezogener Daten qualifiziert werden, die er innerhalb der Nutzung verarbeiten lässt, zumal er über die Zwecke und wesentlichen Mittel der Verarbeitung faktisch entscheidet. Agiert ein KI-System jedoch außerhalb der durch die „Gebrauchsanweisung“[27] determinierten Zweckbestimmung und verarbeitet autonom personenbezogene Daten, die es nicht verarbeiten sollte, stellt sich die Frage, ob und inwiefern der Betreiber auch hierfür verantwortlich ist oder der Anbieter des KI-Systems eine Mitverantwortung trägt. Zu verhindern sind Schutzlücken für betroffene Personen, die aufgrund der Autonomie des Systems entstehen können.[28]

Für eine datenschutzrechtliche **Differenzierung** zwischen dem Einsatz herkömmlicher Software (iSv automatisierter Verarbeitung) und einem KI-System zur (autonomen) Verarbeitung personenbezogener Daten **spricht** auch der **risikobezogene Aspekt**. Neben dem AI Act, der den risikobasierten Ansatz maßgeblich verfolgt, ist datenschutzrechtlich auf nationaler Ebene die **DSFA-V**[29] (Negativliste) zu adressieren. Gem § 2 Abs 2 Z 4 DSFA-V handelt es sich nämlich bei der *„Nutzung oder Anwendung neuer bzw neuartiger Technologien* […], *insb durch den Einsatz von künstlicher Intelligenz“* um eine besonders risikobehaftete Verarbeitung, womit stets die Pflicht zur

[17] Art 3 Z 66 AI Act „*KI-System mit allgemeinem Verwendungszweck*“. [18] ErwGr 100 AI Act. [19] Ebd. [20] Art 4 Z 2 DSGVO. [21] Art 2 Abs 1 DSGVO. [22] *Heißl* in *Knyrim* (Hrsg), DatKomm Art 2 Rz 50, uVa *Jahnel/Bergauer*, DSGVO Art 2 Rz 7. [23] OGH 27. 11. 2019, 6 Ob 150/19f RIS-Justiz RS0132574 [T 2]. [24] *Ennöckl* in *Sydow*, Europäische Datenschutzgrundverordnung² Art 2 Rz 6. [25] Vgl ErwGr 12 AI Act. [26] Art 3 Z 4 AI Act. [27] Art 3 Z 15 AI Act. [28] Lediglich aufgeworfen wird an dieser Stelle der Aspekt, ob es sich bei autonomen KI-Systemen um eine Datenverarbeitung sui generis handelt, was große Konsequenzen für die datenschutzrechtliche Verantwortlichkeit, betroffene Personen als auch die sachliche Anwendbarkeit der DSGVO und DSG zur Folge haben könnte. [29] V der DSB über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) StF BGBl II 2018/278.

Durchführung einer Datenschutz-Folgenabschätzung (DSFA) verbunden ist. Es wird daher bereits auf nationaler Ebene klargestellt, dass es sich bei der Verwendung von KI zur Verarbeitung personenbezogener Daten um eine neuartige, besonders risikobehaftete Verarbeitung handelt, die aufgrund des besonders hohen Risikoniveaus mit dem herkömmlichen Begriff „Verarbeitung" oder „automatisierte Verarbeitung" nicht einfach gleichzusetzen ist, zumal allein durch den Einsatz von KI zur Datenverarbeitung den Verantwortlichen erhöhte Pflichten treffen.

Transparenzpflichten im AI Act sollen der Black-Box-Problematik trotzen.

Ferner funktionieren KI-Systeme bislang als undurchsichtige **„Black Boxes"**, wodurch es massiv an verständlichen Erläuterungen über den Entscheidungsfindungsprozess fehlt. Damit einhergehend leidet auch erheblich die notwendige Transparenz hinsichtlich des Umgangs der damit verbundenen Verarbeitung personenbezogener Daten, was ein systemimmanentes Problem darstellt. Um dieser Problematik entgegenzuwirken, wurden im AI Act diverse **Transparenzpflichten** normiert.[30] Bspw muss nach Art 13 AI Act der Anbieter eines Hochrisiko-KI-Systems einen hinreichend transparenten Betrieb gewährleisten, indem das KI-System so konzipiert sein muss, dass der Betreiber die Ergebnisse des Systems angemessen interpretieren und verwenden kann.

Conclusio

Als „KI-System" iSd AI Act ist ein graduell autonom betriebenes, anpassungsfähiges, maschinengestütztes System zu qualifizieren, das aus Eingaben unterschiedliche Ziele ableitet, die geeignet sind, die Umgebung zu beeinflussen. Im Einsatz von KI-Systeme zur Verarbeitung personenbezogener Daten liegt eine „neue Art" der Datenverarbeitung, denn sie besticht durch graduell abstufbar autonomes Handeln, ist mit hohen Risiken für die Betroffenen verbunden, birgt ein hohes Maß an Intransparenz und ist sohin grds nicht mit der automatisierten Verarbeitung gleichzustellen. Daher resultiert aus der Verwendung von KI zur Verarbeitung personenbezogener Daten stets die Pflicht zur Durchführung einer DSFA.

Dako 2024/26

[30] Art 50 Abs 1, Art 53 AI Act.

Zum Thema

Über den Autor

Moritz W. Rothmund-Burgwall, LL.M., ist Jurist und als Researcher sowie Consultant am Research Institute – Digital Human Rights Center tätig.
E-Mail: moritz.rothmund-burgwall@researchinstitute.at

Hinweis

Die Erstellung dieses Beitrags erfolgte im Rahmen des von der Österreichischen Forschungsförderungsgesellschaft (FFG) geförderten Forschungsprojekts „HYBRIS" (Förderungsnummer 44155055), das Teil des österreichischen Sicherheitsforschungsprogramms KIRAS des Bundesministeriums für Finanzen (BMF) ist.