DATENSCHUTZRECHTLICHE ANFORDERUNGEN AN KI-GESTÜTZTE PLATTFORMEN ZUR KRISENBEWÄLTIGUNG

Thorsten Conrad / Diogo Sasdelli / Nils Wiedemann / Alessia Zornetta

Thorsten Conrad, Studentischer Mitarbeiter, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes
Saarland Informatics Campus C3.1, 66123 Saarbrücken, DE
thorsten.conrad1@uni-saarland.de

Diogo Campos Sasdelli, Wissenschaftlicher Mitarbeiter, Institut für Rechtsinformatik, Universität des Saarlandes
Campus A5 4, 66123 Saarbrücken, DE
diogo.campos_sasdelli@uni-saarland.de

Nils Wiedemann, Wissenschaftlicher Mitarbeiter, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes
Saarland Informatics Campus C3.1, 66123 Saarbrücken, DE
nils_torben.wiedemann@uni-saarland.de

Alessia Zornetta, S.J.D. Candidate, UCLA Institute for Technology, Law & Policy
Charles E Young Dr E, 385, 90095, Los Angeles, CA, US
alessiazornetta@gmail.com

Schlagworte: ***Datenschutzrecht, Online-Plattform, KI-Recht, Krisenbewältigung, Privacy by Design***

Abstract: *Eine wirksame Methode zur Bewältigung von Krisensituationen erfordert eine schnelle Erfassung und Analyse großer Mengen von Daten, sowie eine effiziente Koordination der an der Krisenbewältigung beteiligten Akteure. Mit den technischen Fortschritten der letzten Jahre eröffnet sich die Möglichkeit, hierzu durch künstliche Intelligenz unterstützte Online-Plattformen einzusetzen. Die im Rahmen solcher Plattformen stattfindenden Verarbeitungen personenbezogener Daten fallen in den Anwendungsbereich der DSGVO. In diesem Kontext diskutiert der vorliegende Beitrag ausgewählte datenschutzrechtliche Fragestellungen, insbesondere die Verantwortlichkeit von Plattformbetreibern und -benutzern sowie den Grundsatz von Privacy by Design im Bereich der Krisenbewältigung.*

1. Einleitung und Problemstellung

In Anbetracht jüngster Ereignisse wie der Covid-19-Pandemie, des Halbleitermangels, und der durch den russischen Angriffskrieg gegen die Ukraine verursachten Energie- und Nahrungskrisen wird deutlich, dass die bisherigen Methoden zur Krisenbewältigung nicht ausreichen, um die teils erheblichen Auswirkungen rechtzeitig erkennen und effektiv bewältigen oder gar vermeiden zu können. Solche Krisenszenarien sind äußerst komplexe Situationen, die sich nach den vielfältigsten Faktoren in nahezu unvorhersehbarer Weise weiterentwickeln können. Wirksamere Bewältigungsmaßnahmen erfordern daher, dass (1) große Mengen von Daten (etwa Kontakt- Standort-, Infektions- Energieverbrauchsdaten sowie Echtzeitdaten im Verkehrsbereich oder zur Lage von Lieferketten) schnell erfasst und analysiert werden sowie (2) die Koordination zwischen den an der Krisenbewältigung beteiligten Akteuren (z.B. öffentliche Einrichtungen, Unternehmen) gefördert wird.

Ein Lösungsansatz besteht darin, die an der Krisenbewältigung beteiligten Akteure in eine durch künstliche Intelligenz (KI) unterstützte Online-Plattform zusammenzubringen.[1] Der vorliegende Beitrag diskutiert die

[1] Diesen Ansatz verfolgen die vom BMWK geförderten KI-Projekten zur Krisenbewältigung, wie z.B. PAIRS, SPELL, ResKrVer und CoyPu. Vgl. https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2021/07/20210727-altmaier-ki-kann-krisenmanagement-unterstuetzen.html (15.11.2022).

Struktur und die Funktionsweise solcher *KI-gestützten Plattformen zur Krisenbewältigung* und behandelt ausgewählte datenschutzrechtliche Fragestellungen, die sich in diesem Kontext stellen.

2. KI-gestützte Plattformen zur Krisenbewältigung

Der Lösungsansatz *KI-gestützte Plattform* setzt sich aus zwei Kernelementen zusammen. Das erste Kernelement ist die Struktur einer *Plattform*. Bisher hat sich noch keine einheitliche, allgemeingebräuchliche rechtliche Definition von *Plattform* etablieren können. Nach Spiecker gen. Döhmann zeichnen sich Plattformen dadurch aus, dass sie „auf unterschiedlichen Ebenen [agieren], mindestens verknüpfen sie verschiedene Infrastrukturen, Dienste, Anbieter und Nutzer über ein von ihnen vorgegebenes technisches Format bzw. die technischen Schnittstellen, also durch das Mittel der technischen Standardisierung. Oftmals stellen sie auch selbst Inhalte bereit oder wirken jedenfalls an deren Generierung, Aufbereitung und Verbreitung mit."[2] Sie lassen sich nach ihr als „gleich einer *Spinne im Netz*" beschreiben: „Sie ermöglichen überhaupt erst die Netzwerkstrukturen, sie bilden deren zentralen Knotenpunkt, über den alle Interaktionen und alle Vernetzungen laufen."[3] Eine Plattform führt also Vorgänge zentral zusammen und verbindet die einzelnen Plattformbenutzer untereinander. Dadurch wird die gemeinsame Planung besser koordiniert, so dass erforderliche Maßnahmen schneller ergriffen werden können.

Das zweite Kernelement ist der Einsatz von KI. Auch hier ist keine allgemein anerkannte Definition vorhanden. Russel und Norvig diskutieren bspw. vier Ansätze zur Definition von KI, die schwerpunktmäßig entweder auf der Rationalität oder auf der Menschenähnlichkeit des Verhaltens oder der ‚Denk'-Vorgänge von Maschinen basieren.[4] Bei all diesen Ansätzen spielt die Fähigkeit, sich an neuen Situationen anzupassen bzw. über vorgegebene Lösungsmuster hinauszugehen, eine zentrale Rolle. Maschinen diese Fähigkeit zu verleihen gehört zum Bereich des *Machine Learning*, im Rahmen dessen eine Maschine gemäß eines Lernalgorithmus anhand von Datenmengen (sog. *Trainingsdaten*) programmiert wird. Da insbesondere dieser Aspekt des allgemeinen KI-Begriffes bei der Bewältigung von Krisensituationen vielversprechend erscheint, wird hier unter ‚KI' stets eine nach dem *Machine-Learning*-Ansatz programmierte Maschine verstanden. Dabei ist zwischen den verschiedenen Entwicklungsphasen von KI zu unterscheiden. Laut der deutschen *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder* (DSK) kann man den Lebenszyklus einer KI-Software in (1) Design-, (2) Trainings- und (3) Einsatzphasen unterteilen.[5] In der Designphase werden das KI-System und seine Komponenten erarbeitet. In der zweiten Phase, der Trainingsphase, wird die KI auf der Basis der jeweils gesammelten Daten durch maschinelles Lernen trainiert. Die Einsatzphase stellt die eigentliche Nutzung des KI-Systems dar. Dabei ist festzuhalten, dass die Trainingsphase auch parallel zur Einsatzphase laufen kann, wobei die KI fortlaufend mit den nutzerspezifischen Rohdaten trainiert wird,[6] was aufgrund des dynamischen Charakters ihres Anwendungsbereiches bei den hier zu betrachtenden Plattformen zu erwarten ist. Der Einsatz von KI ermöglicht generell die Erfassung und die Analyse großer Mengen von Daten in dynamischen Szenarien. Im Kontext der Krisenbewältigung können so präzisere Vorhersagen ge-

---

2 Spiecker gen. Döhmann, Digitale Mobilität: Plattform Governance, GRUR 2019, S. 341 (S. 342).

3 Spiecker gen. Döhmann, Digitale Mobilität: Plattform Governance, GRUR 2019, S. 341 (S. 342); vgl. auch die Definition in Bertolini/Episcopo/Cherciu, Liability of online platforms, Brüssel 2021, S. III. Vgl.: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf (15.11.2022).

4 Russel/Norvig, Artificial Intelligente. A Modern Approach, Pearson, Harlow 2022, S. 19 ff.

5 DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen. Vgl.: https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf (15.11.2022); zusammengefasst in Wyderka, DSK: Erste konkrete Vorgaben zu Entwicklung und Betrieb von Künstlicher Intelligenz, ZD-Aktuell 2020, 06928.

6 DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 15.

troffen werden, wodurch rechtzeitig wirksame Maßnahmen ergriffen werden können, um solche Situationen abzumildern oder im Idealfall sogar zu vermeiden.

3. Datenschutzrechtliche Anforderungen

Die zwei Kernelemente dieses Lösungsansatzes sowie der von ihnen verfolgte Zweck der Krisenbewältigung sind mit besonderen datenschutzrechtlichen Anforderungen verbunden.

3.1. Sachlicher Anwendungsbereich der DSGVO

Schwierig gestaltet sich bereits die Frage, ob der sachliche Anwendungsbereich nach Art. 2 DSGVO eröffnet ist. Gemäß Artikel 2 Abs. 1 gilt die DSGVO „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen." Dass bei KI-gestützten Plattformen zur Krisenbewältigung Daten automatisch verarbeitet bzw. in Form von Dateisystemen i.S.v. Art. 4 Nr. 6 gespeichert werden, liegt nach der obigen Beschreibung auf der Hand.

3.1.1. Personenbezogene Daten

Für die Eröffnung des sachlichen Anwendungsbereichs der DSGVO kommt es also darauf an, ob die von solchen Plattformen verarbeiteten Daten *personenbezogene* Daten i.S.v. Art. 4 Nr. 1 sind. Dieser definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen". Für die Bewältigung von Krisensituationen im Gesundheitsbereich wie bspw. der Covid-19-Pandemie kann es für eine präzise Materialbedarfsprognose erforderlich sein, dass Laborwerte analysiert werden, um regionale Ausbrüche frühzeitig erkennen und die Auswirkungen ermitteln zu können. Auch könnten über eine Analyse der Infektionsketten Vorhersagen getroffen, auf deren Basis vorbeugende Maßnahmen ergriffen werden können. Bei der Bewältigung von Krisen im Bereich der Energieversorgung dürfte wiederum für die Generierung von Handlungsempfehlungen erforderlich sein, dass der Energieverbrauch oder einzelne Stromausfälle analysiert werden und insoweit auch Daten über Anschlüsse einzelner Personen verarbeitet werden. In all diesen und in weiteren Fällen handelt es sich um die Verarbeitung von Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen, also um die Verarbeitung personenbezogener Daten i.S.v. Art. 4 Nr. 1 DSGVO.[7] In Bezug auf solche Verarbeitungen wird also der sachliche Anwendungsbereich der DSGVO grundsätzlich eröffnet sein.

Um dieses Ergebnis zu vermeiden, wäre erforderlich, den Personenbezug der verarbeiteten Daten aufzuheben. Dies kann durch Datenanonymisierung erreicht werden. Dabei ist zu beachten, dass der schiere Umstand, dass im Sinne der hier diskutierten Plattformen die Daten bei maschinellen Lernverfahren als Trainingsdaten eingesetzt werden, keineswegs automatisch zur Aufhebung des Personenbezugs führt. Denn obwohl auf den ersten Blick keine Informationen zu einzelnen Personen zu beinhalten scheint, ist es unter Umständen möglich, mit gezielten Angriffen dennoch herauszufinden, ob bzw. mit welcher Wahrscheinlichkeit die Daten einer bestimmten Person Teil der Trainingsdaten waren.[8] Daher gelten für die Anonymisierung von Trainingsdaten besondere Anforderungen, etwa der Einsatz von *State-of-the-Art*-Anonymisierungsmethoden.[9] Allerdings

[7] Möllers, On Privacy in home automation systems, S. 62.

[8] Winter/Battis/Halvani, Herausforderungen für die Anonymisierung von Daten, ZD 2019, S. 489 (S. 492).

[9] Für Anforderungen an die Anonymisierung von Trainingsdaten vgl. etwa Leffer/Leicht, Datenschutzrechtliche Herausforderungen beim Einsatz von Trainingsdaten für KI-Systeme. In: Schweighofer/Saarenpää/Eder/Zanol/Schmautzer/Kummer/Hanke (Hrsg.), Recht DIGITAL – 25 Jahre IRIS. Tagungsband des 25. Internationalen Rechtsinformatik Symposiums IRIS 2022, Editions Weblaw, Bern 2022, S. 89.

wird in manchen Fällen eine ausreichende Anonymisierung praktisch nicht durchzuführen sein,[10] sodass der sachliche Anwendungsbereich der DSGVO eröffnet sein wird.

3.1.2. DSGVO und Katastrophenschutz

Der mit der Plattform verfolgte Zweck der Krisenbewältigung könnte indes dazu führen, dass die DSGVO nach Art. 2 Abs. 2. keine Anwendung findet. In Betracht kommt erstens die Ausnahme bzgl. Verarbeitungen im Rahmen einer Tätigkeit außerhalb des Anwendungsbereichs des Unionsrechts nach Art. 2 Abs. 2 lit. a. DSGVO. Krisenbewältigung und Katastrophenschutz werden primär durch das Recht der Mitgliedstaaten geregelt, weshalb der Union keine Regelungskompetenz zukommen könnte. Überzeugend erscheint indes die Auffassung von Hornung und Stroscher, wonach der Anwendungsbereich des Unionsrechts weit auszulegen sei. Für die Vermeidung der Ausnahme in lit. a) sei ausreichend, wenn die Verarbeitung überhaupt einen Bezug zum Unionsrecht haben kann.[11] Hinzu komme, dass der Union nach Art. 6 lit. f AEUV eine explizite Regelungskompetenz im Bereich des Katastrophenschutzes zuzuordnen ist. Soweit greift Art. 2 Abs. 2 lit. a also nicht ein.

Zweitens kommt die Ausnahme nach Art. 2 Abs. 2 lit. d bzgl. Verarbeitungen durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Lit. d bezieht sich auf die Abgrenzung der DSGVO gegenüber der JI-Richtlinie, deren Anwendungsbereich sich genau auf solche Fälle beschränkt (vgl. Art. 1 Abs. 1 JI-RL). Zwar lässt der Wortlaut der deutschen Fassung der Vorschrift mutmaßen, dass die Bewältigung von Krisensituationen bzw. Katastrophenschutz – als Abwehr von Gefahren für die öffentliche Sicherheit – durch die Ausnahme von Art. 2 Abs. 2 lit. d DSGVO gedeckt, mithin gemäß Art. 1 Abs. 1 JI-RL in den Anwendungsbereich der JI-Richtlinie fallen würde. Diese Ausnahme greift nach überzeugender Meinung von Hornung und Stroscher allerdings ebenfalls nicht ein.[12] Mit „Abwehr von Gefahren für die öffentliche Sicherheit“ sei nämlich nicht jede Form von Gefahrenabwehr gemeint, sondern lediglich die Abwehr von Gefahren im Zusammenhang mit Straftaten.[13]

Somit greift Artikel 2. Abs. 2 nicht ein; der sachliche Anwendungsbereich der DSGVO ist daher eröffnet.

3.2. Verantwortliche und Auftragsverarbeiter

Als Nächstes ist zu prüfen, welche unter den an der Plattform beteiligten Akteuren für entsprechende Datenverarbeitungen als Verantwortliche bzw. als Auftragsverarbeiter anzusehen sind.

3.2.1. Abgrenzung Verantwortlichkeit/Auftragsverarbeitung

Eingangs stellt sich die Frage, ob die einzelnen Plattformbenutzer bzw. der Plattformbetreiber die datenschutzrechtlichen Bedingungen für eine Verantwortlichkeit erfüllen. Die DSGVO unterscheidet in ihrer Systematik zwischen Verantwortlichen und Auftragsverarbeitern. „Verantwortlicher“ ist i.S.v. Art. 4 Nr. 7 DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit

[10] Leffer/Leicht, Datenschutzrechtliche Herausforderungen beim Einsatz von Trainingsdaten für KI-Systeme, S. 90; Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen: Datenschutzrechtliche Voraussetzungen und technische Lösungsansätze, Franz Vahlen, München 2022, S. 1286.

[11] Vgl. Hornung/Stroscher, Datenschutz in der Katastrophe. Anwendbarkeit, Systematik und Kompetenzfragen – Teil 1, GSZ 2021, S. 149 (S. 151).

[12] Vgl. Hornung/Stroscher, Datenschutz in der Katastrophe. Anwendbarkeit, Systematik und Kompetenzfragen – Teil 1, GSZ 2021, S. 149 (S. 151 f).

[13] Vgl. Hornung/Stroscher, Datenschutz in der Katastrophe. Anwendbarkeit, Systematik und Kompetenzfragen – Teil 1, GSZ 2021, S. 149 (S. 151); Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO, Art. 2 Rn. 39. Auf Englisch ist von “*threats to public security*”, nicht von “*public safety*” die Rede.

anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". „Auftragsverarbeiter" ist wiederum gemäß Art. 4 Nr. 8 „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet". Es hängt vom jeweiligen konkreten Fall ab, ob ein datenverarbeitender Akteur ein (gemeinsam) Verantwortlicher oder ein Auftragsverarbeiter ist.

Was die einzelnen Plattformbenutzer betrifft (i.d.R. Regierungsorgane, Unternehmen usw.), kann prinzipiell ausgeschlossen werden, dass sie bloße Auftragsverarbeiter ist, zumal ein Plattformbenutzer in keinem Weisungsverhältnis zum Plattformbetreiber steht. Vielmehr entscheiden sie selbständig, welche personenbezogenen Daten auf welche Weise erhoben, verarbeitet und im Rahmen der Plattform geteilt und weiterverwendet werden sollten. Insofern sind die einzelnen Benutzer grundsätzlich als Verantwortliche anzusehen.

Komplexer gestaltet sich die Lage hinsichtlich der Verantwortlichkeit des Plattformbetreibers. Hierbei erscheint ratsam, zwischen den oben im Abschnitt 2 angeführten KI-Entwicklungsphasen zu unterscheiden. Bei der Trainingsphase wird der Plattformbetreiber als die Entität, die für das Betreiben des KI-Systems zuständig ist, über Mittel und Zweck von Datenverarbeitungen bestimmen, die der Weiterentwicklung dieses Systems dienen. Hierbei ist er also grundsätzlich als Verantwortlicher anzusehen. Bei der Einsatzphase muss wiederum die besondere Natur des von der Plattform verfolgten Ziels berücksichtigt werden: Krisenbewältigung ist eine schwierige Angelegenheit, die als solche die koordinierte und auf die jeweilige Situation angepasste Handlung der beteiligten Akteure erfordert, zu denen auch der Plattformbetreiber gehört. Insofern ist im Regelfall zu erwarten, dass er auch hier über Mittel und Zwecke der entsprechenden Datenverarbeitungen (mit-)entscheiden wird.

Es wäre allerdings denkbar, dass einzelne Plattformbenutzer das KI-System auch für Datenverarbeitungen einsetzen könnten, die jenseits der Bewältigung einer konkreten Krisensituation liegen, etwa für die Durchführung von Analysen von Daten, die in früheren Krisensituationen gesammelt wurden, wodurch dieser Benutzer auf eine Optimierung seiner internen Strukturen abzielt. In solchen besonderen Fällen würde der Plattformbetreiber lediglich nach den Anweisungen des Benutzers handeln. Dann wäre der Benutzer als der Verantwortliche, der Plattformbetreiber wiederum bloß als Auftragsverarbeiter anzusehen.[14]

Aus den obigen Erwägungen ergibt sich, dass sowohl der Plattformbetreiber als auch die einzelnen -benutzer im Regelfall als Verantwortliche anzusehen sind.

3.2.2. Gemeinsame Verantwortlichkeit

Nach der Feststellung ihrer Verantwortlichkeit drängt sich die Frage auf, ob Plattformbetreiber und -benutzer als gemeinsam Verantwortliche anzusehen sind. Legen nämlich zwei oder mehr Verantwortliche *gemeinsam* die Zwecke der und die Mittel zur Verarbeitung fest, so sind diese gemäß Art. 26 Abs. 1 DSGVO gemeinsam Verantwortliche und müssen eine „Vereinbarung in transparenter Form" festlegen.

Wie oben erwähnt, erfordert der von der Plattform verfolgte Zweck, d.h. Krisenbewältigung, dass Plattformbetreiber und -benutzer koordiniert handeln. Insofern ist im Regelfall zu erwarten, dass Entscheidungen über Zweck (Krisenbewältigung) und Mittel (Plattformstruktur und KI-Komponenten) der Datenverarbeitungen gemeinsam zu treffen sein werden. Damit wäre die Bedingung für eine gemeinsame Verantwortlichkeit grundsätzlich erfüllt.

Zwischen Plattformbetreiber und -benutzern besteht dabei insofern eine Asymmetrie, als Letztere lediglich der Plattform beitreten bzw. Mittel und Zweck der Verarbeitung annehmen können. Diese Asymmetrie führt dazu, dass die jeweiligen Entscheidungsbeiträge bzgl. Mittel und Zweck der Verarbeitung hinsichtlich dreier

[14] EDPB Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, S. 27; Quelle: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf (15.11.2022).

Aspekte auseinanderfallen können: (1) Inhalt, (2) Umfang und (3) Zeit.[15] Dabei muss ferner in Bezug auf die KI-Komponenten unterschieden werden, ob es sich hierbei um Verarbeitungen im Rahmen der Trainingsphase oder im Rahmen der Einsatzphase handelt.

Bzgl. Inhalt setzt die gemeinsame Verantwortlichkeit voraus, dass sich die Entscheidungen der gemeinsam Verantwortlichen über Mittel und Zweck der Verarbeitung inhaltlich zumindest teilweise decken.[16] Diese inhaltliche Übereinstimmung ist hier in Bezug auf die Einsatzphase erfüllt; denn Plattformbetreiber und alle Benutzer verfolgen durch den Einsatz von KI als Mittel gemeinsam den Zweck, Krisensituationen zu bewältigen. Bei der Trainingsphase ist die inhaltliche Übereinstimmung ebenfalls erfüllt; denn sowohl der Plattformbetreiber als auch die Benutzer bezwecken die Weiterentwicklung der KI, indem sie ihr die jeweils gesammelten Daten als Trainingsdaten zur Verfügung stellen.

Auch in Bezug auf den Umfang ist hinsichtlich des Verarbeitungszweckes erforderlich, dass alle gemeinsam Verantwortlichen einen gewissen Grad an Übereinstimmung teilen.[17] Hinsichtlich des Mittels ist indes unerheblich, ob alle gemeinsam Verantwortlichen die Verarbeitungsmittel gleichermaßen einsetzen oder nicht. Vielmehr reicht für eine gemeinsame Verantwortlichkeit schon aus, wenn alle Verantwortlichen die Mittel (mit-)bestimmen oder zumindest akzeptieren.[18] Dies ist hier bei Einsatz- und Trainingsphase aufgrund des besonderen Ziels der Krisenbewältigung bzw. der Weiterentwicklung der KI festzustellen. In Bezug auf das Mittel wäre die Teilnahme an der Plattform ausreichend.

Was schließlich den zeitlichen Aspekt betrifft, ist eine Beteiligung bei der Bestimmung von Mitteln und Zwecken von Anbeginn an für die Erfüllung der im Art. 26 Abs. 1 DSGVO vorgesehene Bedingung nicht erforderlich. Stattdessen ist schon ausreichend, dass die zuvor bestimmten Mittel und Zwecke akzeptiert und angenommen werden.[19] Der Zeitpunkt des Entscheidungsbeitrages setzt lediglich die zeitliche Grenze der gemeinsamen Verantwortlichkeit: Ein Plattformbenutzer ist kein Verantwortlicher bzgl. Datenverarbeitungen, die vor seinem Beitritt zur Plattform stattfanden.[20] Problematischer erweist sich demgegenüber die Situation betreffend Verarbeitungen, die nach einem evtl. Austritt eines Benutzers aus der Plattform ereignen würden; denn solange er Beiträge zur Entwicklung der KI geleistet hat, so gilt grundsätzlich, dass die KI nach wie vor einen Rest an von diesem Benutzer zur Verfügung gestellten personenbezogenen Daten beinhalten würde. Daher wäre dieser Benutzer selbst nach seinem Austritt aus der Plattform zumindest im Rahmen der Einsatzphase als gemeinsam Verantwortlicher anzusehen. Diese Sichtweise führte indes zur wohl viel zu harten Folge, dass man nach einer Beteiligung an dem Training eines KI-Systems mit Einsatz von personenbezogenen Daten grundsätzlich dauerhaft den Status eines gemeinsamen Verantwortlichen tragen müsste. Für solche Fälle könnte sich daher als angemessener erweisen, eine Sonderlösung zu finden. In Anlehnung an die Rechtsprechung des EuGH zur Verantwortlichkeit bzgl. einzelner Verarbeitungsphasen könnte mit seinem Austritt i.d.R. die Grundlage für die gemeinsame Verantwortlichkeit hinsichtlich Verarbeitungen, die erst nach dem Austritt erfolgten, entfallen.[21] Dies hätte Auswirkungen insbesondere auf die Ausübung von Betroffenenrechten, da diese dem ausgetretenen Plattformbenutzer gegenüber nicht mehr geltend gemacht werden könnten.

Nach den obigen Erwägungen ist festzuhalten, dass der Plattformbetreiber und die einzelnen Plattformbenutzer sowohl hinsichtlich der Einsatz- als auch der Trainingsphase des entsprechenden KI-Systems im Regelfall als gemeinsam Verantwortliche anzusehen sind.

---

15 Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 24.
16 Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 26.
17 Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 28.
18 EuGH v. 10.7.2018 – C-25/17 (Zeugen Jehovas), Rn. 63–73. Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 27.
19 Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 25.
20 Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 25.
21 EuGH v. 29.07.2019 – C-40/17 (FashionID), Rn. 74; Freund, in: Schuster/Grützmacher, IT-Recht, Art. 26 DSGVO, Rn. 35–38.

3.3. Privacy by Design

Die umfassenden und komplexen Verarbeitungen von Teils personenbezogenen Daten in KI-gestützten Plattformen zur Krisenbewältigung führen zu Konflikten mit dem Datenschutzrecht. Diese Konflikte können durch ein möglichst datenschutzfreundliches Design vermieden werden. Das Ziel sollte ein „eingebauter Datenschutz" sein, also die Erfüllung des Grundsatzes *Privacy by Design*.[22] Dieser ist gesetzlich in Art. 25 DSGVO verankert. Art. 25 Abs. 1 DSGVO verpflichtet die Verantwortliche geeignete technische und organisatorische Maßnahmen so zu treffen, dass „die Datenschutzgrundsätze [...] wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen."

Adressat dieser Verpflichtung ist primär der Verantwortliche. Auftragsverarbeiter werden mittelbar über Art. 28 DSGVO adressiert, nach dem der Verantwortliche keinen Auftragsverarbeiter beauftragen darf, der die notwendigen Garantien des Art. 28 Abs. 1, die auch die Verpflichtung aus Art. 25 Abs. 1 beinhalten, nicht geben kann.[23] Zusätzlich werden Hersteller, die weder Verantwortliche oder Auftragsverarbeiter sind, über die Lieferketten von der Regelung „übers Dreieck" betroffen.[24] Die in Art. 25 DSGVO genannte Verpflichtung gilt für den gesamten Lebenszyklus der Verarbeitung und müssen ständig aktualisiert werden.[25] Der relevante Zeitrahmen reicht von der frühestmöglichen Planungs- und Konzeptionsphase über den gesamten Verarbeitungsprozess hinaus.[26] Der Grundsatz sollte daher so früh wie möglich ausreichend berücksichtigt werden.

Art. 25 Abs. 1 DSGVO umfasst sowohl technische als auch organisatorische Maßnahmen:[27] Explizit wird in Art. 25 DSGVO die Pseudonymisierung als Beispiel genannt. Weitere Beispiele können die Datenaggregation, Anonymisierung, Daten-Dashboards, Software mit offenem Quellcode, Dezentralisierung, Tags und Single-Sign-On-Services sein.[28] Der Verantwortliche muss allerdings nicht über den Stand der Technik hinausgehen. Dieser muss nicht einmal unbedingt erreicht werden,[29] sondern nur neben anderen Faktoren – wie etwa den Implementierungskosten – berücksichtigt werden.[30]

Die Umsetzung des *Privacy-by-Design*-Grundsatzes dürfte dabei sowohl Plattformbetreiber als auch Plattformbenutzer treffen. Neben Standardmaßnahmen werden insbesondere in sensiblen Bereichen, wie dem Gesundheitsbereich, eine Vielzahl an speziellen Maßnahmen zu treffen sein. Ein gemeinsames und koordiniertes Vorgehen der Plattformbeteiligten wird daher für die Erfüllung des Grundsatzes unerlässlich sein.

3.3.1. Unbestimmtheit des Krisenbegriffs und Zweckbindungsgrundsatz

Problematisch für die wirksame Umsetzung der Datenschutzgrundsätze, insbesondere des Zweckbindungsgrundsatzes, könnte das weite Verständnis des Begriffs der Krisenbewältigung sein.

Der Zweckbindungsgrundsatz besagt gemäß Art. 5 Abs. 1 lit. b DSGVO, dass personenbezogene Daten nur für einen festgelegten, eindeutigen und legitimen Zweck erhoben werden dürfen. Der Zweck ist der Fixpunkt für die Rechtfertigungstatbestände und für die Informationspflichten nach Art. 13 ff. DSGVO.[31] Er dient einer Kontrollfunktion und soll die Verarbeitung auf einen überschaubaren Umfang begrenzen.[32] Eine recht-

[22] Baumgartner, in: Ehmann/Selmayr, DS-GVO, Art. 25, Rn. 1.
[23] Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 25 DSGVO, Rn. 25–26.
[24] Hartung, in: Kühling/Buchner, DSGVO, Art. 25 Rn. 13; Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 25 DSGVO, Rn. 25–26.
[25] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 5.
[26] Nolte/Werkmeister, in: Gola/Heckmann, DSGVO, Art. 25, Rn. 13 ff.
[27] Nolte/Werkmeister, in: Gola/Heckmann, DSGVO, Art. 25, Rn. 15 ff.
[28] mit weiteren Beispielen: Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 25 DSGVO, Rn. 29 ff.
[29] Lang, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 25 DSGVO, Rn. 55.
[30] Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 25 DSGVO, Rn. 38 ff.
[31] Schantz, in: Wolff/Brink, Art. 5 DSGVO, Rn. 13.
[32] Herbst, in: Kühling/Buchner, DS-GVO, Art. 5, Rn. 22.

mäßige Verarbeitung ist ohne Beachtung des Zweckbindungsgrundsatzes nicht möglich.[33] Die wirkungsvolle Durchsetzung des Zweckbindungsgrundsatz kann garantiert werden, indem auf technische Maßnahmen wie physische oder logische Trennung der Daten (zum Beispiel nach Bereich) oder besondere Kennzeichnung der Datenkategorien (sog. Tagging) zurückgegriffen wird.[34]

Umstritten ist, wie eindeutig der Zweck bestimmt sein muss, um Art. 5 Abs. 1 lit. b DSGVO zu erfüllen. Eindeutig im Sinne des Art. 5 Abs. 1 lit. b DSGVO ist der Zweck, wenn er sich von anderen Zwecken klar unterscheiden lässt.[35] Der Zweck ist so bestimmt zu fassen, dass er die Verarbeitung in nachvollziehbarer Weise begrenzt.[36] Der Verantwortliche darf die Daten also nicht auf Vorrat für künftige Zwecke erheben, die nicht bekannt und unvorhersehbar sind, beziehungsweise im Nachhinein bestimmt werden.[37]

Nach einem strengen Verständnis ist die Zweckbestimmung grundsätzlich eng zu fassen und erfordert einen präzisen Geschäfts- oder Verwaltungszweck wie einen konkreten Geschäftsakt, ein Verwaltungsverfahren oder ein speziell verfolgtes Interesse.[38] Offene nicht näher beschriebene Zwecke sind nach diesem strengen Verständnis unzulässig.[39] Datenverarbeitungen, bei denen der genaue Zweck noch nicht absehbar ist, widersprechen dem Grundsatz.[40]

Nach einer anderen Ansicht sind umfangreichere Zweckbestimmungen zulässig, wenn der Betroffene über die Ungewissheit aufgeklärt wird und eine Vorstellung davon hat, wie diese Ungewissheit sich am Ende der Verarbeitung auflöst.[41] Eine Datenverarbeitung, bei der das Ergebnis noch nicht gänzlich feststeht, ist also nicht grundsätzlich ausgeschlossen. Der Zweck der Verarbeitung ist nach dieser Ansicht „eindeutig" im Sinne des Zweckbindungsgrundsatzes, wenn die Ungewissheit gerade durch die Verarbeitung aufgelöst werden soll und der Betroffene entsprechend aufgeklärt wurde.[42] Kommt es im Einzelfall zu nicht näher bestimmbaren Zweckbestimmungen bietet die Zweckänderung in Art. 6 Abs. 4 DSGVO entsprechenden Handlungsspielraum.[43]

Die letztgenannte Ansicht überzeugt, da es nach dem Sinn und Zweck der Vorschrift nicht auf eine starre Grenze ankommen sollte. Es sollte vielmehr ausreichend sein, dass der Verarbeitungszweck mindestens so detailliert ist, dass für den Betroffenen erkennbar ist, welche Art. der Datenverarbeitung vorliegt und welche Rechte der Betroffene hat.[44] Dafür braucht es keinen genauen Geschäfts- oder Verwaltungszweck, sondern hinreichende Informationen für den Betroffenen.

Hat der Verantwortliche die personenbezogenen Daten zum Zwecke der Krisenbewältigung erhoben, stellt sich die Frage, ob dieser Zweck eindeutig bestimmt ist. Der Begriff der Krisenbewältigung ist auslegungsbedürftig. Fraglich ist bereits, was eine Krise ist. Nach dem Duden ist eine Krise eine „schwierige Lage, Situation, Zeit [die den Höhe- und Wendepunkt einer gefährlichen Entwicklung darstellt] (...)".[45] Dieser Begriff ist naturgemäß vage, da er die Vielzahl an Krisenszenarien aus verschiedenen Bereichen widerspiegelt.

---

33 Herbst, in: Kühling/Buchner, DS-GVO, Art. 5, Rn. 12.

34 Baumgartner, in: Ehmann/Selmayr, DS-GVO, Art. 25, Rn. 13; Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 25 DSGVO, Rn. 30.

35 Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 DSGVO, Rn. 76.

36 Herbst, in: Kühling/Buchner, DS-GVO, Art. 5, Rn. 35.

37 Heberlein, in: Ehmann/Selmayr, DS-GVO, Art. 5 Rn. 13.

38 Rossnagel/Nebel/Richter, Was bleibt vom Europäischen Datenschutzrecht? – Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, S. 455, (S. 458); Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 DSGVO, Rn. 88 ff.

39 Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841, (S. 1843–1844).

40 Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 DSGVO, Rn. 88.

41 Herbst, in: Kühling/Buchner, DS-GVO, Art. 5, Rn. 22; Herbst, Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD 2016, S. 371, (S. 373).

42 Conraths, Künstliche Intelligenz in der Medienproduktion, MMR 2021, S. 457, (S. 459).

43 Kühling, Gesundheitsdatenschutzrecht im Zeitalter von „Big Data", DuD 2020, S. 182, (S.186); Conraths, Künstliche Intelligenz in der Medienproduktion, MMR 2021, S. 457, (S. 459).

44 Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 6 DSGVO, Rn. 98.

45 https://www.duden.de/rechtschreibung/Krise

So gibt es in vielen (Rechts-) Gebieten Begriffe zu Krisen, wie beispielsweise die „Gasmangellage“ und die „Versorgungskrise“ im Energierecht[46] sowie im Gesundheitsbereich den „Schutz vor Infektionskrankheiten“ und die in der Coronakrise viel beachtete „Überlastung der Gesundheitsversorgung“.[47] Infolgedessen kann in einem bestimmten Bereich eine Krise bestehen, während ein anderer Bereich hierbei nicht betroffen ist.

Der weite Begriff der Krisenbewältigung allein ist nicht ausreichend, um die Ungewissheit im Rahmen der Zweckbestimmtheit aufzulösen. Durch eine Begrenzung der Krisenbewältigung auf bestimmte Bereiche kann dieser Ungewissheit ausreichend Rechnung getragen werden. Die Bestimmung einzelner Gebiete, wie beispielsweise Logistik, Gesundheit oder Energieversorgung, können es der Plattform ermöglichen das Merkmal der Eindeutigkeit und somit den Zweckbindungsgrundsatz zu erfüllen. Es empfiehlt sich ferner, die einzelnen Krisenszenarien genau zu definieren und die Parameter festzusetzen, wie beispielsweise die Überwachung der Lieferketten, um Lieferengpässe zu erkennen und Überwachung von Infektionskrankheiten zur Erkennung von Epidemien.

3.3.2. Vereinbarkeit mit dem Grundsatz der Transparenz

Einen weiteren wichtigen Grundsatz für KI-gestützte Plattformen zur Krisenbewältigung stellt der Transparenzgrundsatz gemäß Art. 5 Abs. 1 lit. a. DSGVO dar. Der Grundsatz enthält die Pflicht, dass für die betroffene Person die Verarbeitung erkennbar ist und sie Informationen über die Risiken der Verarbeitung und ihre Betroffenenrechte erhält.[48] Nach Erwägungsgrund 39 S. 3 sollen Informationen in leicht verständlicher (einfacher) Sprache verfasst werden.[49] Dadurch soll der Betroffene in die Lage versetzt werden, Rechtsverstöße erkennen zu können und seine Betroffenenrechte auszuüben.[50] Bei komplexen KI-Systemen erwächst dabei die Problematik, dass eine verständliche Darstellung der Handlungsweise[51] nur schwer möglich ist.[52] Eine sog. „Blackbox“, also ein KI-System, bei dem nicht einmal der Hersteller den Verarbeitungsvorgang nachvollziehen und erklären kann, ist mit dem Transparenzgrundsatz unvereinbar.[53] Technische und organisatorische Maßnahmen, die diesen Grundsatz durchsetzen sollen, sind ausführliche Datenschutzerklärungen, Einwilligungstexte, sowie KI-spezifisch Zugang zu umfangreichen Dokumentationen der Trainingsphase und der Protokolle um die Nachvollziehbarkeit zu erhöhen.[54]

Für den Bereich der Krisenbewältigung sollen die Betroffenen den technischen Lösungen vertrauen und deren Nutzen akzeptieren.[55] Das wird eher der Fall sein, wenn der Betroffene weiß, wie der Mechanismus funktioniert und dass seine Daten nicht uferlos verarbeitet werden. Ein besonders anschauliches Beispiel dafür ist die Entwicklung der (deutschen) Corona-Warn-App. Sinn und Zweck der App war es, Infektionsketten nachzuverfolgen und zu unterbrechen. Die App wurde mit ihrem dezentralen, datenschutzfreundlichen, Open-Source-Ansatz über 40 Millionen Mal heruntergeladen und erhielt bisher über 11 Millionen Datenspenden.[56] Das ist insbesondere vor dem Hintergrund beeindruckend, dass es anders als bspw. bei der *Luca App* für die

[46] So bspw. im Notfallplan Gas der Bundesrepublik Deutschland, S. 17 ff, abrufbar unter https://www.bmwk.de/Redaktion/DE/Downloads/M-O/notfallplan-gas-bundesrepublik-deutschland.pdf?__blob=publicationFile&v=5 (15.11.2022).

[47] Kiessling, in: Kießling, InfSchG, § 1 InfSchG, Rn. 4 ff.

[48] Reimer, in: Sydow/Marsch, DS-GVO BDSG, Art.5, Rn. 17.

[49] Franzen, in: Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, Art. 5 DSGVO, Rn. 4.

[50] Pötters, in: Gola/Heckmann, DSGVO, Art. 5, Rn. 12; Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 DSGVO, Rn. 50.

[51] Die DSGVO verwendet in Art. 13 und 14 hierfür das Wort „Logik“.

[52] Schürrmann, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, S. 316 (S. 318).

[53] Gausling, Künstliche Intelligenz im digitalen Marketing, ZD 2019, S. 335 (S. 336).

[54] DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 5.

[55] Müller, Nutzung von Mobildaten zur Eindämmung der Pandemie, MMR 2020, S. 355 (S. 359).

[56] Vgl.: https://www.coronawarn.app/de/#privacy sowie https://www.coronawarn.app/de/analysis/ (15.11.2022).

Benutzer keine über die Unterbrechung von Infektionsketten hinausgehende Motivation gab, um die App herunterzuladen, wie beispielsweise die Verschaffung von Zugang zu Restaurants.

4. Schluss

KI-gestützte Plattformen zur Krisenbewältigung stellen einen vielversprechenden Ansatz dar, der vor allem im Bereich des Katastrophenschutzes zur Rettung vieler Menschenleben führen könnte. Die Entwicklung solcher Plattformen unterliegt nicht nur technischen, sondern auch rechtlichen Herausforderungen.

In Bezug auf datenschutzrechtliche Aspekte fallen solche Plattformen in den Anwendungsbereich der DSGVO. Im Regelfall – und vor allem bzgl. Verarbeitungen im Rahmen der Trainingsphase der KI – dürften dabei sowohl der Plattformbetreiber als auch die einzelnen Plattformbenutzer als gemeinsam Verantwortliche i.S.v. Art. 4 Nr. 7 i.V.m. Art. 26 DSGVO anzusehen sein. Bei einem zu starken Auseinanderfallen der Entscheidungsbeiträge bzgl. Mittel und Zweck der Datenverarbeitung, dabei vor allem im Falle des Austritts eines Benutzers aus der Plattform wäre indes denkbar, dass die Verantwortlichkeit dieses Benutzers insoweit begrenzt wird. Hinsichtlich einzelner Verarbeitungen, für die die Plattform von einem jeweiligen Benutzer beauftragt wird, wäre ferner denkbar, dass die Plattform bloß die Rolle eines Auftragsverarbeiters übernähme.

Hinsichtlich des *Privacy-by-Design*-Grundsatzes sollten die Verantwortlichen bei der Verarbeitung von personenbezogenen Daten durch KI-Systeme den datenschutzrechtlichen Herausforderungen, die ihnen die DSGVO beim Verarbeiten personenbezogener Daten stellt, bereits in der Designphase angemessen berücksichtigen. Damit die Anforderungen des Zweckbindungsgrundsatzes erfüllt sind, muss der Zweck so detailliert wie möglich beschrieben werden, damit die Betroffenen angemessen über die Verarbeitung informiert sind. Bei der Krisenbewältigung ist ein Kontext also hinreichend zu bestimmen, um die Parameter der Verarbeitung genau festzulegen. Nur wer genau weiß, wozu er die personenbezogenen Daten verarbeitet, kann Maßnahmen treffen, die auch bei anspruchsvollen Projekten eine datenschutzrechtlich zulässige Verarbeitung ermöglichen. Eine zulässige Verarbeitung schafft Vertrauen in technische und administrative Maßnahmen, was die Krisenbewältigung nachhaltig fördern kann.

5. Danksagung

Dieser Beitrag entstand im Rahmen des Projekts „PAIRS“ (www.pairs-projekt.de, Förderkennzeichen: 01MK21008H), das durch das Bundesministerium für Wirtschaft und Klimaschutz finanziert wird.