48. Jahrgang
datenschutz-berater.de
DSB 12/2024

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Philipp Quiel
Vernünftige Erwartungen Seite 285

Stichwort des Monats

Laurenz Strassemeyer
Ankunft der Widerspruchslösung im Europäischen Case Law Seite 286

Datenschutz im Fokus

Carlo Piltz und Alexander Weiss
Berechtigte Interessen als Rechtsgrundlage für das Training von KI-Modellen Seite 291

Patrick Gsell
Erforderlichkeit von digitalen Optimierungs- und Automatisierungsmaßnahmen Seite 298

Johannes Nehlsen und Tilmann Fleck
Personalaktendaten und Vertraulichkeit: Inwieweit verpflichtet die Verpflichtung? Seite 301

Dominik Küster
Technischer Datenschutz im Jahresbericht 2023 der Berliner Datenschutzbeauftragten Seite 306

Aktuelles aus den Aufsichtsbehörden

Conrad S. Conrad
EDSA: Verpflichtungen bei der Beauftragung von Auftrags- und Unterauftragsverarbeitern Seite 308

Rechtsprechung

Jan Spittka
BGH zu DSGVO-Massenklagen – Alle Klarheiten beseitigt! Seite 311

Prof. Christian Solmecke
BGH zum Facebook-Datenleck: Das Beste kommt zum Schluss Seite 314

Dominik Sorber und Christina Knoepffler
Hören Sie mich? Headsets als mitbestimmungspflichtige, zur Überwachung geeignete Einrichtungen Seite 318

- **Nachrichten** Seite 289

ISSN 0170-7256

dfv Mediengruppe

Carlo Piltz und Alexander Weiss

Berechtigte Interessen als Rechtsgrundlage für das Training von KI-Modellen

Der Einsatz von künstlicher Intelligenz (KI) birgt noch viele ungeklärte Rechtsfragen. Mit dem Inkrafttreten der KI-Verordnung soll unter anderem ein einheitlicher Rechtsrahmen für die Entwicklung von KI-Systemen statuiert werden. Sobald allerdings eine Verarbeitung personenbezogener Daten im Rahmen des Trainings von KI-Modellen stattfindet, ist auch der Anwendungsbereich der DSGVO eröffnet. Bislang umstritten ist die Frage, welcher Erlaubnistatbestand eine solche Verarbeitung zu rechtfertigen vermag. Eine praxistaugliche und rechtssichere Lösung ist essentiell, um die Entwicklung von KI europaweit zu fördern.

Einleitung

KI wird derzeit als thematischer Dauerbrenner in sämtlichen Medien diskutiert. Produkte und Dienstleistungen werden mit dem Schlagwort KI als Alleskönner angepriesen. Generative KI-Modelle, wie GPT-4, LLa. M.a oder Gemini sind in der Lage, selbst Daten zu generieren, und haben sich mittlerweile als fester Bestandteil des Alltags etabliert. Mit dem Inkrafttreten der KI-Verordnung hat sich nun auch der Europäische Gesetzgeber der Thematik gewidmet und die Verwendung und Nutzung von KI-Systemen und -Modellen reguliert. Allerdings fällt die Verwendung von KI-Systemen auch unter bereits bestehende Regularien. Insbesondere die DSGVO ist für Entwickler und Verwender von KI-Modellen relevant, sobald personenbezogene Daten verarbeitet werden. Vertritt man die Auffassung, dass sogenannte Large Language Models (LLMs) als generative KI-Modelle keine personenbezogenen Daten mehr enthalten (vgl. HmbBfDI, Diskussionspapier: Large Language Models und personenbezogene Daten, S. 9), steht zeitlich vorgelagert die Entwicklung von KI-Modellen in Form des Trainings in einem besonderen Fokus der datenschutzrechtlichen Bewertung.

Dieser Beitrag widmet sich der Frage, inwiefern die Verarbeitung personenbezogener Daten beim Training eines KI-Modells als zulässig erachtet werden kann.

Training von KI-Modellen als Datenverarbeitung

Welcher Erlaubnistatbestand des Art. 6 DSGVO die im Rahmen des Trainings eines KI-Modells stattfindenden Verarbeitungen datenschutzrechtlich legitimieren kann, ist ein strittiges Thema. Jüngst hat der EDSA diese Frage auf seine Agenda genommen und eine Stellungnahme gemäß Art. 64 Abs. 2 DSGVO angekündigt, die zuvor von der irischen Aufsichtsbehörde beantragt worden war. In einer im Vorfeld vom EDSA veranstalten Diskussionsrunde mit relevanten Stakeholdern, wurde die Zulässigkeit der Datenverarbeitung für das Training einer KI insbesondere mit der Einwilligung oder auf Basis des berechtigten Interesses des Verantwortlichen begründet.

Generative KI-Modelle werden mit großen Datenmengen trainiert und können Zusammenhänge und Muster in den Datensätzen erkennen und darauf basierend beispielsweise eigene Texte generieren. Die dafür erforderlichen Trainingsdatensätze können beispielsweise Bilder oder Texte sein und personenbezogene Daten enthalten.

Das Training eines KI-Modells lässt sich im Hinblick auf die verwendeten Datensätze in zwei Arten unterteilen: Zum einen können Entwickler für das Training auf eigene Datensätze zurückgreifen, sogenannte First-Party-Data. Zum anderen werden öffentlich verfügbare Daten von Websites Dritter über sogenannte Webcrawler ermittelt und heruntergeladen, um sie anschließend in KI-Modelle zu transferieren, sogenannte Third-Party-Data. Im Rahmen des Trainings einer KI finden grundsätzlich mehrere Verarbeitungsvorgänge statt, nämlich das Herunterladen und Speichern der Datensätze, deren Aufbereitung und schließlich die Verarbeitung im Rahmen des Trainings.

Berechtigte Interesse als zulässige und geeignete Rechtsgrundlage

Faktisch wird sich das Training von KI-Modellen mit personenbezogenen Daten entweder über die Einwilligung der betroffenen Person nach Art. 6 Abs. 1 lit. a) DSGVO oder über die berechtigten Interessen des Verantwortlichen gemäß Art. 6 Abs. 1 lit. f) DSGVO rechtfertigen lassen. Die Verwendung personenbezogener Daten zum Zwecke des Trainings auf Basis eines Vertrages mit Betroffenen (Art. 6 Abs. 1 lit. b DSGVO), dürfte in den seltensten Fällen gelingen, da nach der Rechtsprechung des EuGH diese Verarbeitung objektiv unerlässlich sein müsste, um einen Kernbestandteil des Vertrags zu erfüllen. Dem Verantwortlichen obliegt zudem der Nachweis, dass der Hauptgegenstand des Vertrags ohne die Verarbeitung nicht erfüllt werden kann (EuGH, Urt. v. 04.7.2023 – C-252/21, Rn. 98).

Nachfolgend wird daher der Fokus auf die Einwilligung und die Interessenabwägung gelegt. Die Einwilligung erfordert eine bestätigende Willensbekundung der betroffenen Person im Vorfeld der Verarbeitung ihrer Daten und die Informiertheit der Betroffenen. Demgegenüber setzt Art. 6 Abs. 1 lit. f DSGVO ein legitimes Interesse des Verantwortlichen an der Datenverarbeitung voraus, das mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Personen abzuwägen ist, die nicht überwiegen dürfen. In der Praxis stellt das berechtigte Interesse gegenüber der Einwilligung die vorzugswürdigere Alternative dar.

Argumente gegen die Einwilligung als Rechtsgrundlage

Denn gegen die Einwilligung als Erlaubnistatbestand sprechen vielerlei Gründe. Damit eine Einwilligung überhaupt wirksam sein kann, müssen die Voraussetzungen des Art. 4 Nr. 12 und Art. 7 DSGVO erfüllt sein. Zweifelhaft dürften bei der Verwendung von personenbezogenen Daten zum Training des KI-Modells die konkreten Verarbeitungszwecke für dessen künftige Verwendung sein, die zum Zeitpunkt der Eingabe der Datensätze in das KI-Modell zumeist noch nicht feststehen werden. Aus denselben Gründen wird eine transparente Darstellung der zwingenden Informationen im Einwilligungstext schwierig sein. Darüber hinaus müsste die Einwilligung gemäß Art. 7 Abs. 1 DSGVO bereits vor Beginn der Datenverarbeitung und damit zeitlich vor dem Auslesen mittels Webcrawler eingeholt werden. Dies wird in der Praxis schon häufig daran scheitern, dass es faktisch nicht möglich ist, sämtliche zu den erlangten Datensätzen gehörenden Personen zu ermitteln und zu kontaktieren.

Auch das Vorliegen einer konkludenten Einwilligung lässt sich rechtlich wohl nicht generell begründen. Zwar nennt ErwGr. 32 Satz 2 zur DSGVO ausdrücklich auch Verhaltensweisen als Form einer eindeutig bestätigenden Handlung, sodass z. B. die auf einer Website veröffentlichten personenbezogenen Daten mit Verweis auf den Erlaubnistatbestand in Art. 9 Abs. 2 lit. e DSGVO als konkludente Einwilligung in die Verarbeitung dieser Daten angesehen werden könnten. Ein solcher Erst-Recht-Schluss für eine Rechtfertigung nach Art. 6 Abs. 1 lit. a DSGVO überzeugt jedoch nicht. Denn weder wird das Kriterium der öffentlichen Zugänglichmachung in der DSGVO im Zusammenhang mit der Einwilligung erwähnt noch wären in einem solchen Fall die zwingenden tatbestandlichen Voraussetzungen einer gültigen Einwilligung erfüllt. Zudem hat jüngst der EuGH entschieden, dass durch die Veröffentlichung von Daten nicht auch eine Einwilligung erteilt wird (EuGH, Urt. v. 4.10.2024, C-446/21).

Schließlich ist auch die praktische Umsetzung des Widerrufsrechts der betroffenen Person aus Art. 7 Abs. 3 Satz 1 DSGVO eine faktische Hürde. Zum einen fordert Art. 7 Abs. 3 Satz 4 DSGVO eine ebenso einfache Ausübung, wie die Erteilung der Einwilligung, was bei Third-Party-Data voraussetzt, dass Betroffene wissen, an welchen Verantwortlichen sie sich zu wenden haben und wie sie ihr Recht auf Widerruf ausüben können. Hierzu gilt der bereits oben erwähnte Aspekt der Unmöglichkeit einer Ermittlung sämtlicher betroffener Personen, was die erforderliche Informationserteilung ebenfalls ausschließt. Zum anderen ist die Konsequenz eines ausgeübten Widerrufs, dass die Verarbeitung fortan nicht mehr stattfinden darf, sofern der Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann. In der Folge ist ggf. jede weitere Nutzung der zu Trainingszwecken erworbenen Daten durch das KI-Modell unzulässig. Dementsprechend müssten die betroffenen Datensätze in dem Modell identifiziert und anschließend entfernt werden. Da die Arbeitsweise eines KI-Modells jedoch häufig selbst für Entwickler eine Blackbox ist, gestaltet sich die vollständige Entfernung einzelner Informationen einer konkreten betroffenen Person als die sprichwörtlich bekannte Suche nach der Nadel im Heuhaufen. Doch selbst wenn die betroffenen Daten identifiziert und gelöscht werden könnten, würden die Funktionsfähigkeit und Qualität des KI-Modells unter der Datenlöschung leiden. Letztlich bestünde damit das Risiko, dass der hohe finanzielle und zeitliche Investitionsaufwand infolge eines Widerrufs konterkariert werden würde. Im Ergebnis ist die Einwilligung keine praktikable Rechtsgrundlage für das Training eines KI-Modells. Über dem wirtschaftlichen und gesellschaftlichen Wert des Modells würde stets das Damoklesschwert der wirksamen Erteilung und des Widerrufs der Einwilligung schweben. Dies würde zu einer enormen Beschränkung der Entwicklung und des Betriebs von KI-Modellen führen, was die Wettbewerbs- und Innovationsfähigkeit des Wirtschaftsstandorts Europa massiv beeinträchtigen würde und nicht im Einklang mit den Zielen des Europäischen Gesetzgebers steht.

Zuweilen wird auch argumentiert, dass die Einwilligung als Rechtsgrundlage vorrangig gegenüber den restlichen Erlaubnistatbeständen des Art. 6 Abs. 1 DSGVO sei und Verantwortliche in bestimmten Verarbeitungskonstellationen verpflichtet seien, eine Einwilligung der betroffenen Personen einzuholen. De lege lata resultiert kein Vorrang der Einwilligung gegenüber den übrigen Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO. Die Vorschrift konstituiert keine Privilegierung der Einwilligung, sondern nennt sie gleichrangig neben den übrigen Erlaubnistatbeständen. Ebenso nimmt ErwGr. 40 zur DSGVO auf die Gleichrangigkeit der einzelnen Tatbestandsvarianten des Art. 6 Abs. 1 DSGVO Bezug. Gegen einen Vorrang der Einwilligung hat sich auch der EuGH eindeutig positioniert und dargelegt, dass auch bei fehlender oder unwirksamer Einwilligung ein berechtigtes Interesse als taugliche Rechtsgrundlage in

Betracht kommen kann. In der Entscheidung Meta gegen Bundeskartellamt (EuGH, Urt. v. 4.7.2023 – C-252/21) hat der EuGH zudem ausdrücklich erwähnt, dass es gerade kein Rangverhältnis unter den Erlaubnistatbeständen des Art. 6 Abs. 1 DSGVO gibt.

Berechtigte Interessen des Verantwortlichen für das Training des KI-Modells

Rechtlich zulässig kann die Verarbeitung von personenbezogenen Daten für das Trainieren von KI-Modellen auf Basis der berechtigten Interessen des Entwicklers und von Dritten nach Art. 6 Abs. 1 lit. f DSGVO sein. Dieser Erlaubnistatbestand fordert ein legitimes Interesse des Verantwortlichen und Dritten, die Erforderlichkeit der Datenverarbeitung zur Erreichung dieses Interesses sowie nicht überwiegende Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Person als drei kumulative Voraussetzungen.

Als berechtigtes Interesse zählt jedes rechtliche, wirtschaftliche oder ideelle Interesse. Wirtschaftliche Interessen sind nach herrschender Meinung anerkannt und darüber hinaus nach Art. 16 GRCh geschützt (EuGH, Urt. v. 4.10.2024 – C-621/22). Die Verwendung von KI-Modellen zum Anbieten von verbesserten Produkten oder Funktionalitäten für die Nutzer eines Dienstes kann ebenfalls als ein berechtigtes Interesse gelten, wie etwa bereits der LfDI Baden-Württemberg und die französische CNIL bestätigt haben. Verstöße gegen etwaige Rechtsnormen, wie z. B. die Verwendung verbotener KI-Systeme als Verletzung von Art. 5 Abs. 1 KI-VO, zählen hingegen nicht als ein legitimes Interesse.

Des Weiteren muss die Datenverarbeitung zur Wahrung des berechtigten Interesses erforderlich sein, sodass keine alternativen gleich geeigneten Mittel zu dessen Verwirklichung, wie beispielsweise die Verwendung weniger personenbezogener Daten, in Frage kommen dürfen. In Einzelfällen dürfte die Verarbeitung besonderer Kategorien personenbezogener Daten zum Training eines Hochrisiko-KI-Systems erforderlich sein, um Verzerrungen zu erkennen und zu korrigieren, wobei die Voraussetzungen von Art. 10 Abs. 5 KI-VO i. V. m. Art. 9 Abs. 2 lit. g DSGVO erfüllt sein müssten.

Im Rahmen der Interessenabwägung dürfen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen nicht überwiegen, wobei verschiedene Faktoren miteinzubeziehen sind. Maßgeblich wird der Umfang der Datenverarbeitung sowie die Auswirkungen auf die betroffenen Personen sein. Bei dem Training eines KI-basierten Chatbots für die Beantwortung von Kundenanfragen in einem sozialen Netzwerk werden vermutlich Datensätze einer hohen Anzahl betroffener Nutzer verwendet. Allerdings dürften sich die Datensätze vorwiegend auf bereits gestellte Anfragen an den Kundensupport beschränken und keine spezifischen Informationen über einzelne Nutzer, wie deren Profilfotos, Vorlieben oder Benutzernamen enthalten. Wenn die Daten entsprechend vorgefiltert werden, würde dies gegen eine dateninvasive Verarbeitung sprechen. Im Rahmen der Abwägung wird es somit häufig auf entsprechende technische Maßnahmen zur Risikomitigierung ankommen, um die Interessenabwägung zugunsten des Verantwortlichen begründen zu können.

Für den Verantwortlichen vorteilhaft werden sich auch Interessen des Gemeinwohls, wie der Einsatz eines KI-Modells zur Forschung oder zum Schutz von Grundrechten auswirken. Denn Art. 6 Abs. 1 lit. f DSGVO erlaubt ausdrücklich, auch die berechtigten Interessen von Dritten mit in die Abwägung einzubeziehen. Eine automatisierte Moderation und Inhaltsprüfung durch ein KI-Modell zur Identifizierung und Filterung potenzieller Falschmeldungen oder Hate Speech, dient dem Schutz der Nutzer einer Online-Plattform und ist somit ein gewichtiges Argument für die Annahme eines berechtigten Interesses des Verantwortlichen. Gleiches gilt für die Entwicklung frei zugänglicher KI-Modelle und die Veröffentlichung des Programmcodes auf Diensten (wie Github) wovon letztlich die Allgemeinheit profitieren kann, da dies zur Förderung von vertrauenswürdiger KI beitragen kann.

Neben den häufig angeführten Gefahren für Rechte und Freiheiten betroffener Personen aufgrund des großen Umfangs der Datenverarbeitungen und mangelnder Transparenz über die konkreten Funktionalitäten und Verarbeitungen von KI-Modellen darf nicht außer Acht gelassen werden, dass bei deren Verwendung nicht nur datenschutzrechtliche Aspekte, sondern gemäß Art. 52 Abs. 1 GRCh auch Faktoren, wie die Meinungs- und Informationsfreiheit zu berücksichtigen sind. KI-Modelle können hierzu einen erheblichen Beitrag leisten, deren Potenzial aktuell sicherlich noch nicht vollständig greifbar ist. Gleichwohl kann KI bereits heute beispielsweise Personen mit ähnlichen Interessen auf sozialen Netzwerken miteinander verbinden oder bei der Identifizierung von Falschmeldungen unterstützen.

Ein gewichtiges Argument im Rahmen der Interessenabwägung sind insbesondere die vernünftigen Erwartungen der betroffenen Personen bezüglich der Verarbeitungen, ErwGr. 47 Satz 1 zur DSGVO. Zwar ließe sich vor allem bei der Nutzung von Third-Party-Data argumentieren, dass die auf einer Unternehmensseite veröffentlichten Mitarbeiter nicht damit rechnen werden, dass ihre Fotos samt Namen für das Training einer KI verwendet werden. Dem lässt sich allerdings entgegnen, dass das Abstellen auf rein subjektive Erwartungen nicht sachgerecht erscheint, sondern diese vielmehr durch die Erwartungshaltung eines objektiven

Dritten ergänzt werden. Dass bei im Internet veröffentlichten Daten von einer Verwendung durch Dritte auszugehen ist, scheint eher nah- als fernliegend. Demnach ließe sich auch noch ein Auslesen der Daten durch Webcrawler sowie deren weitere Verwendung unter die vernünftigen Erwartungen subsumieren. Die gleiche Argumentation lässt sich erst Recht auf First-Party-Data übertragen, da registrierte Nutzer eines sozialen Netzwerks von weiteren Verarbeitungen ihrer Daten durch den Betreiber ausgehen dürften. Diesbezüglich wird allerdings relevant sein, inwiefern die betroffenen Personen über eine solche Datenverarbeitung informiert werden, da hier aufgrund der Direkterhebung die Informationspflicht des Art. 13 DSGVO zum Tragen kommen wird.

Als ein weiteres bedeutsames Kriterium sind die Auswirkungen der Datenverarbeitung für die betroffenen Personen zu berücksichtigen. Die Verarbeitung personenbezogener Daten wird bei generativen KI-Modellen (sofern man die Ansicht des HmbBfDI hinsichtlich des fehlenden Personenbezugs vertritt) lediglich im Rahmen des Trainings erfolgen. Denn innerhalb des KI-Modells wird der Personenbezug durch die Tokenisierung aufgehoben. Dementsprechend entstehen aufgrund der anfänglichen Verarbeitung im Rahmen des Trainings keine nennenswerten Risiken für die Rechte und Freiheiten betroffener Personen. Des Weiteren folgt aus dem Umstand, dass insbesondere bei LLMs wegen der Vielzahl der vorhandenen Daten unterschiedlichster Personen die Wahrscheinlichkeit eines Rückschlusses auf eine einzelne Person minimiert wird.

Problematische Konstellationen, die sich zulasten des Verantwortlichen bei der Interessenabwägung auswirken könnten, sind die Verarbeitungen von Daten Minderjähriger oder die Umsetzung von Betroffenenrechten. Ersteres ließe sich durch erweiterte Schutzmaßnahmen, wie beispielsweise enger gefasste Verarbeitungszwecke und einer konsequenten Datenminimierung im Rahmen der Auswahl der Datensätze oder der Verwendung von pseudonymen Daten realisieren. Empfehlenswert wären auch Filterungsmaßnahmen, um auszuschließen, dass solche Datensätze in die KI-Modelle gelangen. Im Hinblick auf Third-Party-Data könnte im Vorfeld bereits auf das Scraping von Websites verzichtet werden, deren Angebot sich an Minderjährige richtet. Denn aufgrund der besonderen Schutzbedürftigkeit von Minderjährigen würde eine Interessenabwägung vermutlich eher zulasten des Verantwortlichen ausfallen. Die Wahrnehmung von Betroffenenrechten stellt Entwickler von KI-Modellen vor großen Herausforderungen. Insbesondere das Recht auf Berichtigung gemäß Art. 16 DSGVO ist aufgrund der Fehleranfälligkeit von KI-Modellen relevant, beispielsweise wenn der generierte Output personenbezogene Daten enthält, die allerdings unrichtig sind. Eine mögliche Maßnahme wäre hier ein Nachtraining des KI-Modells mit den korrigierten Daten oder auch die Anpassung des Algorithmus zur Vermeidung des Fehlers. Jedoch erscheint die Praktikabilität solcher Korrekturen aufgrund des hohen finanziellen und zeitlichen Aufwands zweifelhaft, sodass Filterungen zur Verhinderung des unrichtigen Outputs eine vorzugswürdigere Option sein könnten. Hinsichtlich des Rechts auf Widerspruch nach Art. 21 DSGVO könnten betroffene Nutzer bei First-Party-Data-Sachverhaltskonstellationen ein Opt-Out vor dem Beginn des Trainings erteilen. Bezüglich der Verarbeitung von Third-Party-Data wird sich der Entwickler eines KI-Modells z. B. im Falle des Scrapings von Daten gegebenenfalls auf Art. 11 Abs. 2 Satz 2 i. V. m. Art. 11 Abs. 1 und Art. 12 Abs. 2 Satz 2 DSGVO berufen und argumentieren können, dass die Betroffenenrechte (zumindest Art. 15 bis 20 DSGVO) aufgrund der Unmöglichkeit einer Identifizierung der betroffenen Personen nicht anwendbar sind, sofern die entsprechenden Voraussetzungen erfüllt sind.

Ein weiteres Problem könnte die Verarbeitung besonderer Kategorien personenbezogener Daten sein, da beim Scraping auch sensible Daten, z. B. zur Gesundheit oder zur sexuellen Orientierung, verarbeitet werden können. Als Ausnahmetatbestand käme die offensichtliche Veröffentlichung der Daten durch die betroffenen Personen (Art. 9 Abs. 2 lit. e DSGVO) sowie die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses (Art. 9 Abs. 2 lit. g DSGVO) in Betracht. Der EuGH hat bereits entschieden, dass sich Suchmaschinenbetreiber im Rahmen eines Antrags auf Auslistung von Links zu Inhalten mit sensiblen Daten auf diese Ausnahmetatbestände berufen können (vgl. EuGH Urt. v. 24.9.2019 – C-136/17; EuGH Urt. v. 13.5.2014 – C-131/12). In vielen Fällen wird es sich um offensichtlich öffentlich gemachte Daten der betroffenen Personen handeln, sodass die Ausnahme aus Art. 9 Abs. 2 lit. e DSGVO als zulässig erachtet werden kann. Weiterhin kann sich der Entwickler eines KI-Modells auf Art. 9 Abs. 2 lit. g DSGVO berufen und darlegen, dass das Training der KI unbedingt erforderlich ist, um die in Art. 11 GRCh verankerte Informationsfreiheit der Internetnutzer zu schützen, die ein Interesse daran haben, generative KI-Modelle zu nutzen. Im Gegensatz zur Listung eines Links zu einer Website mit sensiblen personenbezogenen Daten wiegt zugunsten des Entwicklers eines KI-Modells der Eingriff in die Rechte der betroffenen Person deutlich geringer. Denn nach Eingabe der Daten in das KI-Modell wird der Personenbezug entfernt und zudem dürften sich Anfragen an das KI-Modell im Zusammenhang mit der Generierung von Output durch Nutzer vor allem auf Personen des öffentlichen Lebens beziehen. Dementsprechend dürfte die Argumentation des erheblichen öffentlichen Interesses für die Verarbeitung von besonderen Kategorien personenbezogener Daten beim Training einer KI leichter zu begründen sein als für die Verarbeitung im Rahmen des Listings durch Suchmaschinenbetreiber.

Unterscheidung zwischen First- und Third-Party-Data

Die Unterschiede bei der Herkunft der Daten dieser zwei verschiedenen Datensätze wirkt sich nicht auf die Bewertung des berechtigten Interesses aus. Bei Daten, die der Verantwortliche eigenständig erhoben hat, wird er regelmäßig eine Beziehung zu den betroffenen Personen haben, beispielsweise wenn er als Betreiber einer Online-Plattform die Profildaten von seinen Nutzern im Rahmen des Registrierungsprozesses erhoben hat. Bereits dieser Umstand wirkt sich gemäß ErwGr. 47 Satz 2 zur DSGVO positiv auf die Begründung eines berechtigten Interesses aus. Zudem bestehen für den Verantwortlichen weitaus mehr Möglichkeiten, die Betroffenenrechte zu erfüllen, indem er den betroffenen Personen z. B. unmittelbar die erforderlichen Informationen nach Art. 13 DSGVO zur Verfügung stellt oder über das Kundenkonto Prozesse zum Widerspruch oder der Datenlöschung implementieren kann. Wenn ein Verantwortlicher die Daten auf Websites Dritter erhebt, fehlt ihm die unmittelbare Beziehung zu den betroffenen Personen, im Zweifel wird er die einzelnen Personen faktisch gar nicht erst ermitteln können. Die Verarbeitung von Third-Party-Data aber deshalb per se als nicht von Art. 6 Abs. 1 lit. f DSGVO umfasst anzusehen, überzeugt nicht. Die bereits oben angeführten Aspekte zu den tatbestandlichen Voraussetzungen des Art. 6 Abs. 1 lit. f DSGVO zeigen, dass auch Konstellationen im Zusammenhang mit Third-Party-Data unter diesen Erlaubnistatbestand subsumiert werden können. Ferner ist eine Beziehung zwischen dem Verantwortlichen und den betroffenen Personen keine tatbestandliche Voraussetzung. Wäre das Merkmal der Datenherkunft das ausschlaggebende Kriterium für das Vorliegen des berechtigten Interesses, würden sich Wertungswidersprüche auftun, wenn die übrigen tatsächlichen Gegebenheiten identisch wären, aber nur die Verarbeitung von First-Party-Data nach Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt wäre. Dies gilt umso mehr vor dem Hintergrund, dass eine Einwilligung in beiden Konstellationen nicht praktikabel sein wird und die Verwendung von Third-Party-Data folglich datenschutzrechtlich unzulässig wäre.

Auswirkungen beim Training der KI ohne/mit einer ungültigen Rechtsgrundlage

Sofern das Training eines KI-Modells ohne oder mit einer unwirksamen Rechtsgrundlage erfolgt ist, stellt sich die Frage, inwiefern sich dieser Umstand auf die Nutzung des KI-Modells sowie auf etwaige Datenverarbeitungen im Nachgang auswirkt. Etwa bei der Nutzung des nicht-rechtskonformen Systems durch Dritte,. In den USA, aus der die „Fruit of the poisonous tree"-Doktrin stammt, hat ein kalifornisches Gericht die Nutzung eines mit rechtswidrig erlangten Daten trainierten KI-Modells als verboten eingestuft. Die DSGVO hingegen statuiert ein solches Nutzungsverbot nicht unmittelbar.

Auswirkungen von Verstößen beim Scraping auf das Training der KI

Jedoch folgt aus den in Art. 5 Abs. 1 DSGVO genannten Datenschutzgrundsätzen, wie dem Grundsatz der Rechtmäßigkeit oder der Zweckbindung, dass personenbezogene Daten stets nur aufgrund einer gültigen Rechtsgrundlage verarbeitet und die Verarbeitungszwecke geltendes Recht nicht verletzen dürfen. Das führt dazu, dass z. B. bei dem rechtswidrigem Scraping einer Website aufgrund des Urheberrechtsverstoßes (etwa bei dem Außerachtlassen eines zulässig erklärten Nutzungsvorbehalts durch den Betreiber der ausgelesenen Website) für die Erhebung der personenbezogenen Daten zu Trainingszwecken keine Rechtsgrundlage bestünde. Im Hinblick auf das berechtigte Interesse hat der EuGH kürzlich entschieden, dass Verstöße des Verantwortlichen gegen andere aus der DSGVO resultierenden Pflichten sein berechtigtes Interesse an der Verarbeitung entfallen lassen. Hinsichtlich der gescrapten Daten lässt sich in vielen Fällen allerdings anführen, dass es sich um Daten handelt, die für jedermann öffentlich zugänglich und ohne Überwindung technischer Zugangsbeschränkungen abrufbar sind. Diese Auffassung hat auch das LG Detmold vertreten, wonach eine Erhebung dieser Daten weder unbefugt noch unrechtmäßig sei, wenn die betroffene Person durch Vornahme entsprechender Privatsphäre-Einstellungen die Daten öffentlich zugänglich gemacht hat (LG Detmold, Urt. v. 28.3.2023 – 02 O 85/22). Dementsprechend dürfte in solchen Fällen eine Verarbeitung personenbezogener Daten auf Grundlage des berechtigten Interesses zulässig sein. Sofern im Rahmen des Scrapings allerdings Schutzvorkehrungen überwunden und dadurch Rechtsverstöße begangen werden, entfällt auch das berechtigte Interesse des Verantwortlichen und die Verarbeitung jener personenbezogenen Daten beim Training des KI-Modells wäre rechtswidrig.

Allgemeine Verwendung des KI-Modells

Allerdings ist zunächst zu prüfen, ob die DSGVO auf ein KI-Modell, welches auf Basis von rechtswidrigen Datenverarbeitungen entwickelt wurde, überhaupt Anwendung findet. Nach Art. 2 Abs. 1 DSGVO ist nämlich eine Verarbeitung personenbezogener Daten notwendig, damit die DSGVO anwendbar ist. Ein entwickeltes KI-Modell, das auf dem Markt bereitgestellt wird, enthält nach hier vertretener Ansicht allerdings aufgrund der Tokenisierung keine personenbezogenen Daten mehr. Insofern ließe sich argumentieren, dass die DSGVO schon gar nicht anwendbar ist, wenn es auf dem Markt bereitgestellt und von einem Dritten erworben wird.

Eigene Datenverarbeitungen durch Dritte

Bei der Generierung eines Outputs mit personenbezogenen Daten durch den Nutzer des KI-Modells als Dritter bräuchte dieser seinerseits eine gültige Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Mittelbar dürfte die „Fruit of the

poisonous tree"-Doktrin dann zur Anwendung gelangen, wenn sich der Nutzer als Verantwortlicher bei dieser Weiterverarbeitung ebenfalls auf das berechtigte Interesse berufen möchte, da der ursprünglich begangene Rechtsverstoß weiterhin zulasten der betroffenen Personen fortwirken und somit deren Interessen, Rechte und Grundfreiheiten eine höhere Gewichtung erfahren würden. Die CNIL weist darauf hin, dass ein Verantwortlicher der einen veröffentlichten Datensatz nutzen möchte, sicherstellen muss, dass der rechtswidrige Datensatz nicht gegen die DSGVO oder andere Rechtsnormen verstößt. Da die Anbieter der bekanntesten KI-Modelle sich für die Bereitstellung ihrer Anwendungen zur Verwendung durch dritte Unternehmen und Entwickler als Nutzer gegenüber diesen als Auftragsverarbeiter betrachten, würden die Voraussetzungen des Art. 28 Abs. 1 DSGVO gelten. Insofern müssten die kommerziellen Nutzer als Verantwortliche dafür Sorge tragen, dass die Verarbeitung im Einklang mit der DSGVO erfolgt, und nur mit Auftragsverarbeitern zusammenarbeiten, die hierfür auch hinreichende Garantien bieten. Daraus würden Prüfpflichten des Verantwortlichen resultieren. Der EuGH stellt allerdings klar, dass der Verantwortliche für die in seinem Namen erfolgenden Verarbeitungen verantwortlich ist, die durch einen Auftragsverarbeiter durchgeführt werden, wobei der Grundsatz u. a. dann durchbrochen wird, wenn der Auftragsverarbeiter die Daten für eigene Zwecke verarbeitet (EuGH, Urt. v 5.12.2023 – C-683/21, Rn. 84 ff.). Das Training eines KI-Modells durch den Entwickler dürfte einen eigenen Zweck darstellen, der losgelöst von einer Auftragsverarbeitung im Rahmen der Nutzung zu betrachten ist. Dementsprechend dürfte es in einer solchen Konstellation vertretbar sein, eine Zurechnung dieses Verstoßes abzulehnen, sofern für den Endnutzer keine Anhaltspunkte für eine rechtswidrige Datenverarbeitung bestehen.

Aber auch abseits einer möglichen Auftragsverarbeitung im Verhältnis des Nutzers und des Anbieters eines KI-Systems gibt es weitere Argumente, die gegen eine Zurechnung des Rechtsverstoßes des Anbieters als Entwickler des KI-Modells sprechen: Zum einen erhält der Erwerber zunächst ein KI-Modell, das keine personenbezogenen Daten enthält. Zum anderen stellt der Umstand, dass er dann neue Daten eingibt oder durch die Generierung eines Outputs eine Datenverarbeitung in Gang setzt, für sich genommen keinen Verstoß dar, wenn er in diesem Zusammenhang die datenschutzrechtlichen Vorgaben einhält. Insbesondere ließe sich für diese neue Verarbeitung die berechtigten Interessen des Verantwortlichen an der Verwendung des KI-Modells zu den jeweiligen Zwecken als Rechtsgrundlage anführen. Der ursprünglich durch den Entwickler des KI-Modells begangene Rechtsverstoß beim Training dürfte der Legitimation durch Art. 6 Abs. 1 lit. f DSGVO nicht entgegenstehen. Denn der beim Training des Modells begangene Rechtsverstoß ist mit dem Zeitpunkt der Eingabe der Daten in das KI-Modell sowie der dabei stattfindenden Tokenisierung beendet, da der Personenbezug der Trainingsdaten aufgehoben wird. Dementsprechend überwiegen diesbezüglich auch nicht die Interessen, Rechte und Grundfreiheiten der betroffenen Personen, weil aufgrund der zwischenzeitlichen Anonymisierung und der Vielzahl der Datensätze keine nennenswerten Risiken für eine einzelne betroffene Person resultieren. Demgegenüber würde die Versagung der Verwendung eines rechtswidrig trainierten KI-Modells durch den Erwerber eine unverhältnismäßige Einschränkung seiner unternehmerischen Freiheit aus Art. 16 GRCh bedeuten.

Fazit

Die Verarbeitung personenbezogener Daten beim Training eines KI-Modells ist ein umstrittenes Thema, was zum einen an den komplexen technischen Abläufen bei dessen Training und zum anderen an den noch vielen ungeklärten datenschutzrechtlichen Fragestellungen liegt. Es bleibt abzuwarten, ob und inwiefern die Stellungnahme des EDSA Lösungsansätze präsentieren wird. Feststeht hingegen, dass ein praxistaugliches Ergebnis notwendig ist, um die Rechtsunsicherheit für Anbieter und Nutzer zu beseitigen und die Entwicklung von KI-Anwendungen nachhaltig zu fördern. Die anerkannte datenschutzrechtliche Zulässigkeit des Trainings von KI-Modellen auf Grundlage des berechtigten Interesses würde hierzu einen essentiellen Beitrag leisten.

Autoren: **Dr. Carlo Piltz ist Rechtsanwalt bei Piltz Legal in Berlin und spezialisiert im nationalen und internationalen Datenschutzrecht.**

Alexander Weiss ist Rechtsanwalt bei Piltz Legal in Berlin und spezialisiert auf das Datenschutz- und IT-Sicherheitsrecht.